John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
402 W. Broadway, Suite 1760
San Diego, CA 92101
Telephone: (858) 209-6941
Email: jnelson@milberg.com

Attorney for Plaintiff Brian Tash and the Putative Class

UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF CALIFORNIA

BRIAN TASH on behalf of himself and all others similarly situated,

Plaintiff,

v.

VISION SERVICE PLAN a/k/a VSP GLOBAL, VSP VENTURES, LLC, VSP VENTURES MANAGEMENT SERVICES, LLC, and VSP VENTURES OPTOMETRIC SOLUTIONS, LLC,

Defendants.

Case No.

CLASS ACTION COMPLAINT FOR:

1. **VIOLATIONS OF CAL. PENAL CODE § 631, *et seq.*;**
2. **VIOLATIONS OF CAL. PENAL CODE § 638.51(a);**
3. **VIOLATIONS OF CAL. CIV. CODE § 56, *et seq.*;**
4. **VIOLATIONS OF CAL. BUS. & PROF. CODE § 17200, *et seq.*;**
5. **VIOLATIONS OF CAL. CONST. ART. 1 § 1;**
6. **VIOLATION OF THE ELECTRONIC PRIVACY ACT, 18 U.S.C. § 2510, *et seq.***
7. **INTRUSION UPON SECLUSION;**
8. **PUBLICATION OF PRIVATE FACTS; AND**
9. **BREACH OF CONFIDENCE.**

JURY TRIAL DEMANDED

Plaintiff Brian Tash ("Plaintiff") brings this class action complaint ("Complaint") on behalf of himself and all others similarly situated (the "Class Members") against Vision Service Plan a/k/a VSP Global and VSP Ventures, (collectively "VSP" or "Defendant"), which: (1) is the largest vision insurance provider in the United States; (2) partners with doctors and practice groups to provide coverage and discounted services; and (3) operates, controls, and manages several medical facilities. Defendant owns and controls VSP.com, chooseVSP.com, visioncare.vsp.com, VSPdirect.com, and related webpages (the "Website"), and it also owns and controls a mobile app (the "App")(collectively the "Web Properties"). The allegations contained herein, which are based on Plaintiff's knowledge of facts pertaining to himself and his own actions and counsels' investigations, and upon information and belief as to all other matters, are as follows:

NATURE OF THE ACTION

1. Plaintiff brings this class action lawsuit to address VSP's outrageous, illegal, and widespread practice of disclosing its patients confidential personally identifiable information ("PII") and protected health information ("PHI") (collectively referred to as "Private Information") to unauthorized third parties, including Meta Platforms, Inc. d/b/a Meta ("Facebook" or "Meta"), Google LLC ("Google"), LinkedIn (which is owned by Microsoft), and additional unknown data brokers.

2. VSP's unauthorized disclosures of Private Information occurred and continues to occur because of the tracking technologies VSP installed on its Web Properties, including but not limited to the Facebook Pixel, Facebook SDK, Facebook Conversions API, Google Analytics, Google Tag Manager, DoubleClick (owned by Google), LinkedIn's marketing tools, and related tracking tools (collectively, "Tracking Technologies" or "Tracking Tools").

3. The Tracking Technologies allow unauthorized third parties to intercept the contents of patients' communications, receive and view patients' Private Information, mine it for purposes unrelated to the provision of healthcare, and further monetize it to deliver targeted advertisements to specific individuals.

4. VSP owns and controls the Web Properties, which it encouraged Plaintiff and other patients to use for: (1) coordinating their care; (2) obtaining information about their upcoming treatments, therapies, and procedures; (3) identifying in-network providers that meet their unique search criteria; (4) using online calculators to determine their "Cost and Coverage;" (5) enrolling in vision insurance; (6) comparing insurance plans; (7) completing referral requests, forms, quizzes, and other types of dynamic forms; (8) making online payments; and (9) registering for their vision insurance account.

5. In doing so, and by designing its Web Properties in the manner described throughout this complaint, VSP knew or should have known that its patients would use the Web Properties to communicate Private Information in conjunction with obtaining and receiving medical services and insurance from VSP.

6. Plaintiff and other Class Members who used VSP's Web Properties reasonably believed they were communicating only with their trusted healthcare and insurance provider, and nothing about the Web Properties' appearance indicated that unauthorized third parties—Meta, Google, and LinkedIn—would intercept and obtain Private Information submitted by patients.

7. Unbeknownst to Plaintiff and Class Members, however, the Tracking Technologies embedded on VSP's Web Properties contain source code that surreptitiously track, record, and disseminate Plaintiff's and Class Members' online activity and communications (including Private Information) to Meta, Google, and LinkedIn without first obtaining permission, in violation of HIPAA, state laws, industry standards, and patient expectations.

8. By installing and using Tracking Technologies on its Web Properties, VSP effectively planted a bug on Plaintiff's and Class Members' web browsers and devices, which caused their communications to be intercepted, accessed, viewed, and captured by third parties in real time, as they were communicated by patients, based on VSP's chosen parameters.

9. For example, VSP used the Meta Pixel, which "tracks the people and [the] type of actions they take"[1] in real time as they interact with a website, including the exact text and phrases that patients typed into various portions of the Web Properties. Operating as designed and as implemented by VSP, the Meta Pixel and other Tracking Tools caused Plaintiff's and Class Members' Private Information to be unlawfully intercepted and surreptitiously disclosed to third parties.

10. The Office for Civil Rights at HHS has issued a Bulletin to highlight the obligations of HIPAA covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies ("tracking technologies"), such as the Tracking Technologies.[2] The Bulletin expressly provides (in bold type) that "**[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.**" In other words, HHS has expressly stated that VSP's implementation of Tracking Technologies violates HIPAA Rules.

11. The information VSP divulged to unauthorized third-parties—Meta, Google, and LinkedIn—allowed those entities to learn that specific individuals were patients seeking and receiving

///

[1] *See, e.g.*, Facebook, *Retargeting*, https://www.facebook.com/business/goals/retargeting (last visited Oct. 20, 2024)(explaining how the pixel tracks and transmits website users' interactions and communications, allowing for individualized retargeting and marketing.

[2] *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. DEPT. OF HEALTH & HUMAN SERV., https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited Oct. 20, 2023).

treatment at VSP's vision clinics and other medical centers. In and of itself, this reveals the fact that an individual is being treated for vision problems and has received or will receive vision services. In turn, this information was used and/or sold to additional unauthorized parties for use in marketing and geotargeting.

12. Patients simply do not anticipate that their trusted healthcare and insurance provider will send their Private Information to social media and marketing companies for future exploitation and targeted marketing.

13. Neither Plaintiff nor any other Class Member signed a written authorization permitting VSP to send their Private Information to Meta, Google, or LinkedIn.

14. Similarly, VSP does not have a HIPAA-compliant Business Associate Agreement in place with Meta, Google, or LinkedIn.

15. In response to the use of Tracking Technologies by HIPAA covered entities, like VSP, the recently issued HHS Bulletin warns that:

> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule. [3]

16. And as noted by the Hon. William J. Orrick in a decision concerning the use of the

///

[3] *Id.*

Facebook Pixel by healthcare organizations,

> "[o]ur nation recognizes the importance of privacy in general and health information in particular: the safekeeping of this sensitive information is enshrined under state and federal law. The allegations against Meta are troubling: Plaintiff raise potentially strong claims on the merits and their alleged injury would be irreparable if proven."[4]

17. Consequently, Plaintiff brings this action for legal and equitable remedies to address and rectify the illegal conduct and actions described herein, to enjoin VSP from making similar disclosures of its patients' Private Information in the future, and to require VSP to fully articulate, *inter alia*, the specific Private Information it disclosed to third parties and to identify all the recipients of that information.

18. As a result of VSP's conduct, Plaintiff and Class Members have suffered numerous injuries, including invasion of privacy, loss of benefit of the bargain, diminution of value of the Private Information, statutory damages, and the continued and ongoing risk to their Private Information.

19. Plaintiff seeks to remedy these harms and bring causes of action for (1) violations of Cal. Penal Code § 631, *et seq.*; (2) violations of Cal. Civ. Code § 56, *et seq.*; (3) violations of Cal. Bus. & Prof. Code § 17200, *et seq.*; (4) violations of Cal. Const. Art. 1 § 1; (5) violation of the Electronic Communications Privacy Act 18 U.S.C. § 2510, *et seq.*; (6) intrusion upon seclusion; (7) publication of private facts; and (8) breach of confidence.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction under 28 U.S.C. § 1332(d) (the Class Action Fairness Act) because the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and a member of the Class is a citizen of a different state than VSP. This Court also has subject matter jurisdiction under 28 U.S.C. § 1331 because this action arises under 18 U.S.C. § 2510, et seq. (the

///

[4] *In re Meta Pixel Healthcare Litig.*, No. 22-CV-03580-WHO, 2022 WL 17869218, at *1 (N.D. Cal. Dec. 22, 2022).

Electronic Communications Privacy Act).

21. This Court has supplemental jurisdiction over the state law claims under 28 U.S.C. § 1367 because the state law claims form part of the same case or controversy under Article III of the United States Constitution.

22. This Court has personal jurisdiction over Defendant because its corporate headquarters is located in this District.

23. Venue is proper in this District because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

THE PARTIES

24. Plaintiff Brian Tash is an adult citizen and resident of the State of California and is domiciled in Moorpark, California.

25. Vision Service Plan is headquartered in Rancho Cordova, California, and it is the largest vision insurance provider in the United States.

26. VSP Ventures, LLC is a Delaware limited liability company owned and operated by Vision Service Plan. On information and belief, VSP Ventures, LLC is headquartered in this District.

27. VSP Ventures Management Services, LLC is a Delaware limited liability company owned and operated by Vision Service Plan. On information and belief, VSP Ventures Management Services, LLC is headquartered in this District.

28. VSP Ventures Optometric Solutions, LLC is a Delaware limited liability company owned and operated by Vision Service Plan. On information and belief, VSP Ventures Optometric Solutions, LLC is headquartered in this District.

///

///

///

FACTUAL ALLEGATIONS

A. Background

i. Background of California Invasion of Privacy Act

29. The California Legislature enacted the California Invasion of Privacy Act ("CIPA") to protect the privacy rights of California citizens. In doing so, the California Legislature expressly recognized that "the development of new devices and techniques for the purpose of eavesdropping upon private communications … has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." Cal. Penal Code § 630.

30. CIPA prohibits aiding or permitting another person to willfully—and without the consent of all parties to a communication—read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from or received at any place within California.

31. To establish liability under CIPA, Plaintiff need only establish that VSP does, or did, any of the following:

> Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system; or
>
> Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state; or
>
> Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or
>
> Aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

32. Violations of CIPA are not limited to phone lines, but also apply to "new technologies" such as computers, the Internet, and email.[5]

33. CIPA affords a private right of action to any person who has been subjected to a violation of the statute to seek injunctive relief and statutory damages of $5,000 per violation, regardless as to whether they suffered actual damages. Cal. Penal Code § 637.2(a)(1).

34. Moreover, CIPA § 638.51(a) proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

35. A "pen register" is a "device or process that records or decodes dialing, reouting, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

36. By contrast, a "trap and trace device" is a "device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." *Id.*

37. A "pen register" is a "device or process" that records outgoing information, whereas a "trap and trace device" is a "device or process" that recording incoming information.

38. Although CIPA was enacted before the creation of the Tracking Technologies discussed in this Complaint, "the California Supreme Court regularly reads statutes to apply to new technologies where such a reading would not conflict with the statutory scheme." *In re Google Inc*. 2013 WL 5423918, at *21 (N.D. Cal. Sep. 26, 2013); *see also, e.g., Shah v. Fandom, Inc*, --- F. Supp. 3d ---, 2024 WL 4539577, at

[5] *See In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' internet browsing history).

*21 (N.D. Cal. Oct. 21, 2024) (finding trackers similar to those at issue here were "pen registers" and noting "California courts do not read California statutes as limiting themselves to the traditional technologies or models in place at the time the statutes were enacted"); *Mirmalek v. Los Angeles Times Communications LLC*, 2024 WL 5102709, at *3-4 (N.D. Cal. Dec. 12, 2024) (same); *Moody v. C2 Educ. Sys. Inc.*--- F. Supp. 3d ---, 2024 WL 3561367, at *3 (C.D. Cal. July 25, 2024) ("Plaintiff's allegations that the TikTok Software is embedded in the Website and collects information from visitors plausibly falls within the scope of §§ 638.50 and 638.51."); *Greenley v. Kochava, Inc.*, 684 F. Supp. 3d 1024, 1050 (S.D. Cal. 2023) (referencing CIPA's "expansive language" when finding software was a "pen register"); *Javier v. Assurance IQ*, LLC, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) ("Though written in terms of wiretapping, [CIPA] Section 631(a) applies to Internet communications."). This accords with the fact that, "when faced with two possible interpretations of CIPA, the California Supreme Court has construed CIPA in accordance with the interpretation that provides the greatest privacy protection." *Matera v. Google Inc.*, 2016 WL 8200619, at *19 (N.D. Cal. Aug. 12, 2016).

39. Individuals may bring an action against the violator of any provision of CIPA, including § 638.51, for $5,000 per violation. Cal. Penal Code § 637.2(a)(1).

ii. Background of the Confidentiality of Medical Information Act

40. Pursuant to the California Confidentiality of Medical Information Act ("CMIA"), "A provider of health care . . . shall not disclose medical information regarding a patient of the provider of health care . . . without first obtaining an authorization, except as provided in subdivision (b) or (c)." § 56.10(a). "An authorization for the release of medical information . . . shall be valid if it:

> (a) Is handwritten by the person who signs it or is in a typeface no smaller than 14-point type.
>
> (b) Is clearly separate from any other language present on the same page and is executed by a signature which serves no other purpose than to execute the authorization.
>
> (c) Is signed and dated . . .

> (d) States the specific uses and limitations on the types of medical information to be disclosed.
>
> (e) States the name or functions of the provider of health care, health care service plan, pharmaceutical company, or contractor that may disclose the medical information.
>
> (f) States the name or functions of the persons or entities authorized to receive the medical information.
>
> (g) States the specific uses and limitations on the use of the medical information by the persons or entities authorized to receive the medical information.
>
> (h) States a specific date after which the provider of health care, health care service plan, pharmaceutical company, or contractor is no longer authorized to disclose the medical information.
>
> (i) Advises the person signing the authorization of the right to receive a copy of the authorization.

Cal. Civ. Code § 56.11.

41. Moreover, a health care provider that maintains information for purposes covered by the CMIA is liable for negligent disclosures that arise as the result of an affirmative act—such as implementing a system that records and discloses online patients' personally identifiable information and protected health information. Cal. Civ. Code § 56.36(c).[6] Similarly, if a negligent release occurs and medical information concerning a patient is improperly viewed or otherwise accessed, the individual need not suffer actual damages. Cal. Civ. Code § 56.36(b).

42. "In addition to any other remedies available at law, any individual may bring an action against any person or entity who has negligently released confidential information or records concerning them in violation of this part, for either or both of the following: [¶] (1) ... nominal damages of one

///

[6] "Every provider of health care ... who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein. Any provider of health care ... who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36." (§ 56.101, subd. (a).)

thousand dollars ($1,000). To recover under this paragraph, it shall not be necessary that the Plaintiffs suffered or was threatened with actual damages. [¶] (2) The amount of actual damages, if any, sustained by the patient." *Sutter Health v. Superior Ct.*, 227 Cal. App. 4th 1546, 1551 (2014) (quoting Cal. Civ. Code § 56.36(b)).

iii. Meta's Business Tools and the Pixel

43. Meta operates the world's largest social media company and generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[7]

44. In conjunction with its advertising business, Meta encourages and promotes entities and website owners, such as Defendant, to utilizes its "Business Tools" to gather, identify, target, and market products and services to individuals.

45. Meta's Business Tools, including the Pixel and Conversions API, are bits of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of mobile app and website visitors' activity.

46. One such Business Tool is the Pixel, which "tracks the people and type of actions they take."[8] When a user accesses a webpage hosting the Pixel, their communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Meta's servers.

47. Notably, these transmissions to Meta do not occur unless the webpage or mobile app contains the Meta Pixel or another Meta Business Tool. Stated differently, Plaintiff's and Class Members' Private Information would not have been disclosed to Meta but for VSP's decision to install and use Meta Business Tools on its Web Properties.

---

[7] *Facebook, Meta Reports Fourth Quarter and Full Year 2021 Results*, FACEBOOK, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited April 25, 2023).

[8] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting. (Last visited April 25, 2023).

48. These secret transmissions to Meta are initiated by VSP's source code concurrently with Plaintiff's and Class Members' communications to their intended recipient, VSP.

B. VSP Assisted Third Parties in Intercepting Patients' Communications with its Web Properties and Disclosed Plaintiff's and Class Members' Private Information to Third Parties.

49. VSP's Web Properties are accessible on mobile devices and desktop computers and allow patients to communicate with VSP regarding their past, present, and future health care, as well as their past, present, and future medical bills, insurance coverage, and payments.

50. VSP encouraged patients to use the Web Properties to communicate their private information, acquire insurance, identify in-network healthcare providers based on the specific treatment or services they are interested in, schedule appointments, access information about their insurance coverage, pay bills, view records, and more.

51. Despite this, VSP purposely installed Tracking Technologies on its Web Properties and programmed them to surreptitiously share its patients' private and protected communications, including Plaintiff's and Class Members' PHI and PII, which was sent to Meta, Google, Microsoft, and additional third parties.

52. The Tracking Technologies intercepted, recorded, and disseminated patients' information as they navigated and communicated with VSP via the Web Properties, simultaneously and invisibly transmitting the substance of those communications to unintended and undisclosed third parties.

53. The information the Tracking Technologies allowed to be intercepted and received by third parties constitutes Private Information and includes the following:

(a) medical information patients requested or viewed;

(b) information entered into the "Find a Doctor" form and webpage, including the user's street address, which type of physician the user is seeking treatment from ("optometrist" or

"ophthalmologist"), the types of services they are seeking (such as "Laser Vision Care" or "Vision Therapy"), the name of the provider, the vision products sought (such as "Low Vision" or "Hard-to-Fit Contacts"), and more;

(c) the title of any buttons they clicked (such as the "Schedule a Consultation" button, which also indicates that the user is seeking Lasik vision services);

(d) additional search parameters, including the exact text and phrases users typed into text boxes and forms (such as "I want Lasik services" or "I have glaucoma"), the user's street address, the name of their physician, the name of their physician's practice, and more;

(e) selections made from drop-down menus that indicate employer information, insured status, and more (such as "I'm here because I'm a Medicaid member" coupled with "I would like to Find an in-network doctor");

(f) outbound clicks and their corresponding URLs or additional information (such as when users click on their physician's webpage or phone number)

(g) additional sensitive and confidential information made for the provision of obtaining or receiving vision insurance and/or plan benefits, the divulgence of which is and was highly offensive to Plaintiff.

54. The information collected and disclosed by VSP's Tracking Tools is not anonymous and is viewed and categorized by the intercepting party on receipt.

55. The Private Information intercepted by and disclosed to third parties includes identifying information that allows those third parties to know exactly whose information they have acquired.

56. For example, the information Meta received via the Tracking Tools was linked and connected to patients' Facebook profiles (via their Facebook ID or "c_user id"), which includes other identifying information.

57. Similarly, Google "stores users' logged-in identifier on non-Google website in its logs. Whenever a user logs-in on non-Google websites, whether in private browsing mode or non-private browsing mode, the same identifier is associated with the data Google collects from the user's browsing activities on that website. Google further logs all such data (private and non-private) within the same logs and uses these data for serving personalized ads."

58. Simply put, the health information that was disclosed via the Tracking Tools is personally identifiable and was sent alongside other persistent identifiers such as the patients' IP address, Facebook ID, and device identifiers.[9,10]

59. As described by the HHS Bulletin, this is protected health information (PHI) even if the visitor has no previous relationship with VSP because "the information connects the individual to the regulated entity (*i.e.*, it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care."[11]

a. Meta Received Plaintiff's and Class Members' Private Information via Tracking Technologies Installed on VSP's Web Properties.

60. VSP utilized Meta's Business Tools and intentionally installed the Pixel, SDK, Conversions API, and related Meta Business Tools on its Web Properties.

///

[9] *See Brown v. Google, Inc.*, *Brown v. Google LLC*, 525 F. Supp. 3d 1049 (N.D. Cal. 2021) (citing internal evidence from Google employees). Google also connects user data to IP addresses; IP addresses have been classified by the United States Department of Health and Human Services ("HHS") as personally identifying information. *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. Dept of Health and Hum. Servs. (Dec. 1, 2024), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

[10] https://developers.facebook.com/docs/meta-pixel/ (last accessed May 5, 2024).

[11] *See* HHS Bulletin § *How do the HIPAA Rules apply to regulated entities' use of tracking technologies?*

61. This is evidenced by VSP's unique Meta marketing identifiers (represented as "id=24407434961961," "id=2440743496136143," and "id= 492699627863616") that can be used to identify which of its webpages contain the Pixel.[12]

62. Meta's Business Tools allow VSP to optimize the delivery of ads, measure cross-device conversions, create custom audiences (for future targeting marketing and advertising), and decrease its advertising and marketing costs. However, VSP's Web Properties do not require the Pixel to function. Instead, VSP used the Meta Pixel to barter patients' data in exchange for the "free" advertising services offered by Meta.

63. Plaintiff and Class Members never consented, agreed, authorized, or otherwise permitted VSP to disclose their Private Information to Meta, nor did they intend for Meta to be a party to their communications (many of them highly sensitive and confidential) with VSP.

64. VSP's Pixel and Conversions API sent non-public Private Information to Meta, including but not limited to information about Plaintiff's and Class Members' past, present, or future health or health care. *See Supra* ¶45.

65. Importantly, the Private Information Meta received was sent alongside Plaintiff's and Class Members' IP address, Facebook ID (c_user cookie or "FID"), and other persistent device identifiers.

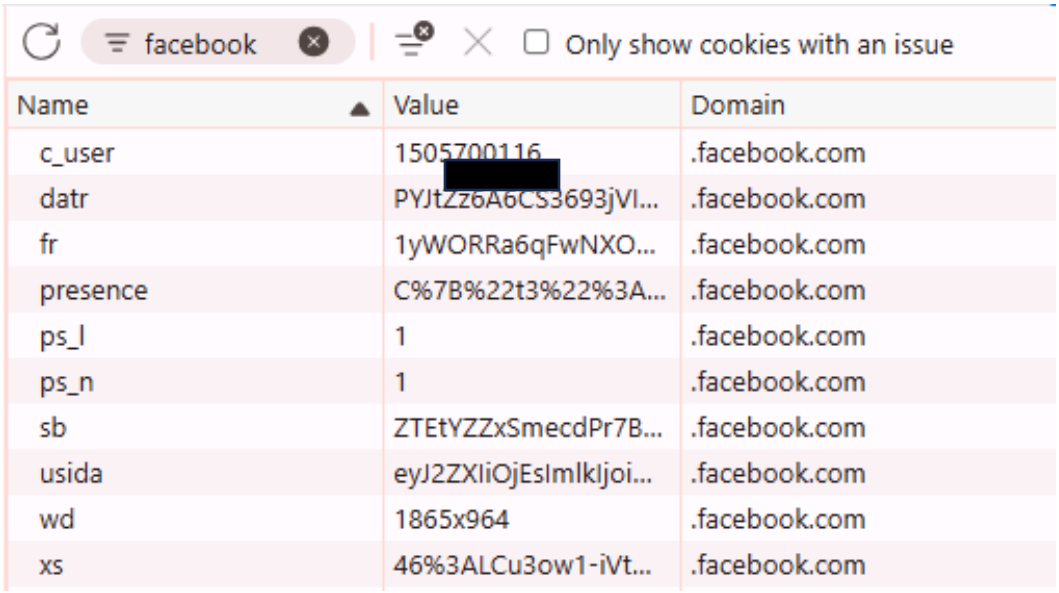
66. The Facebook ID itself is sufficient to link an individual patient's Private Information to their unique Facebook account, real identity, and any other information in Meta's possession. Because a Facebook ID uniquely identifies an individual's account, Meta—or any ordinary person—can easily use it to locate, access, and view the corresponding profile.

///

///

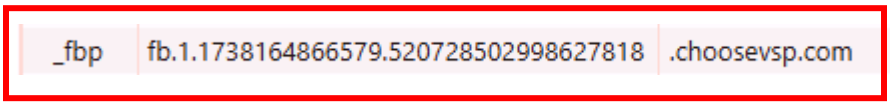
[12] Plaintiff is not presently aware of each and every unique pixel ID associated with and used by VSP and its affiliates on the Web Properties.

67. If a user accessed Defendant's Web Properties from a device where they previously logged into Facebook, their Facebook ID was transmitted to third parties in the form of a c_user cookie that contains the user's unencrypted FID.



68. Importantly, Meta can also identify users that have never created a Facebook, Instagram, or WhatsApp account, but a smaller set of cookies is transmitted to Facebook in these instances.

69. Additionally, VSP also utilizes the _fbp cookie on its Web Properties, which attaches to a browser as a first-party cookie, and which Facebook uses to identify a browser and a user.[13]



70. The Pixel uses both first- and third-party cookies, and both were used on the Web Properties.[14] Notably, it is nearly impossible for website users to block first-party cookies such as the

///

///

[13] *Id.*

[14] A first-party cookie is "created by the website the user is visiting"—in this case, Defendant's Website. A third-party cookie is "created by a website with a domain name other than the one the user is currently visiting"—i.e., Facebook. The _fbp cookie is always transmitted as a first-party cookie. At a minimum, Facebook uses the fr, _fbp, and c_user cookies to link website visitors' data to their to Facebook IDs and corresponding accounts.

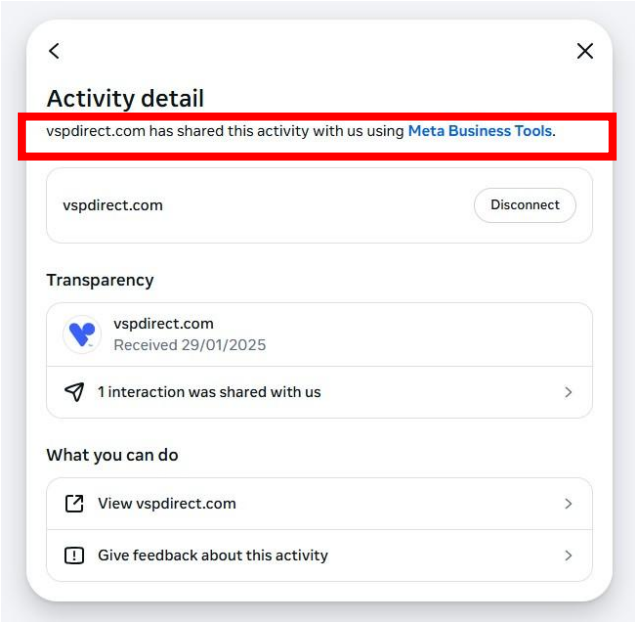
_fbp cookie. Doing so requires specialized knowledge and tools, and often results in the website not functioning properly.

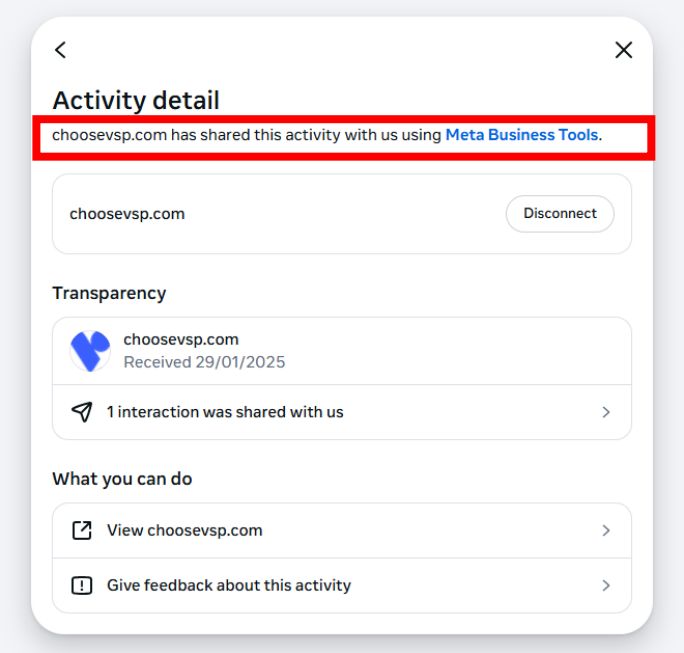
71. Stated differently, even individuals who take extra steps to safeguard their privacy by using ad blockers and blocking third-party cookies cannot prevent VSP's dissemination of their information to Meta.

72. Plaintiff's and Class Members' web browsing activities and communications also are improperly disclosed to Meta via Meta's Conversions API tool.

73. Much like the Pixel, these server-to-server communication are invisible to ordinary users. Additionally, without the opportunity for discovery, it is impossible to know exactly what VSP divulges to Meta because those communications do not emanate from the website user's browser, but instead are sent directly to Meta from VSP's own server.

74. The images below, which were gathered from a user's Facebook account after using a portion of the Web Properties, clearly demonstrate VSP's Web Properties have shared information with Meta, stating "choosevsp.com has shared this activity with us using Meta Business Tools" and "vspdirect.com has shared this activity with us using Meta Business Tools."





75. The full breadth of VSP's tracking and data sharing practices is unclear, but other evidence suggests it used multiple Tracking Technologies that transmitted Private Information to additional third parties.

b. Google and Additional Third Parties Received Plaintiff's and Class Members' Private Information via Tracking Technologies Installed on VSP's Web Properties.

76. The images below demonstrate that Google also received patients' Private Information via the Google Analytics tool, Google Tag Manager, and related tools that communicate with Google Ad Services and DoubleClick, all of which were installed on VSP's Web Properties.

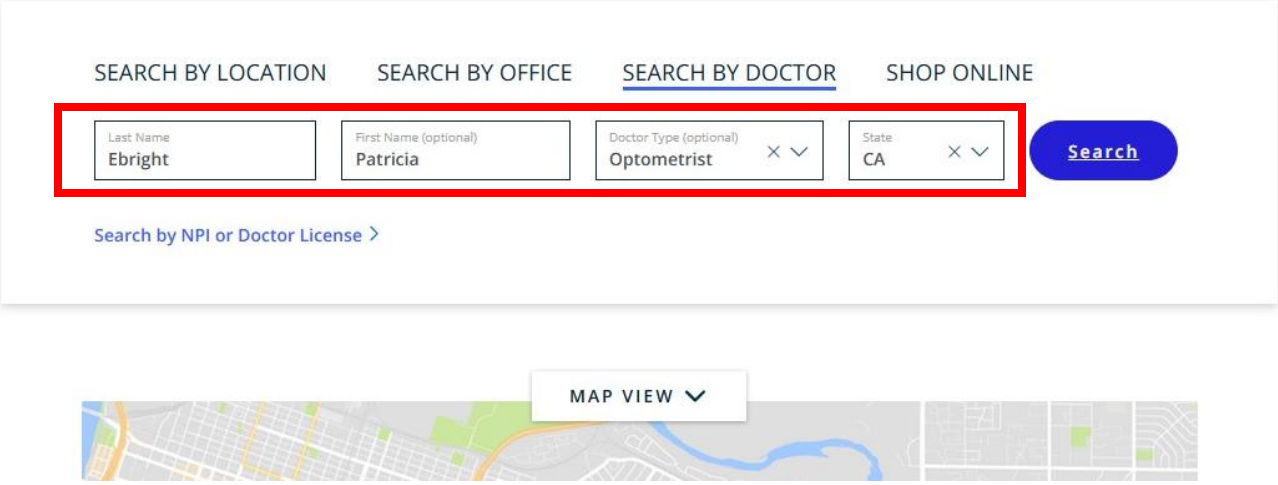
77. When a user interacts with the Web Properties to identify a physician or schedule an appointment by using the "Search by Doctor" tool, they type their physician's name, select the "Doctor Type" from the drop down menu provided, and select the state where the physician is located.

///

///

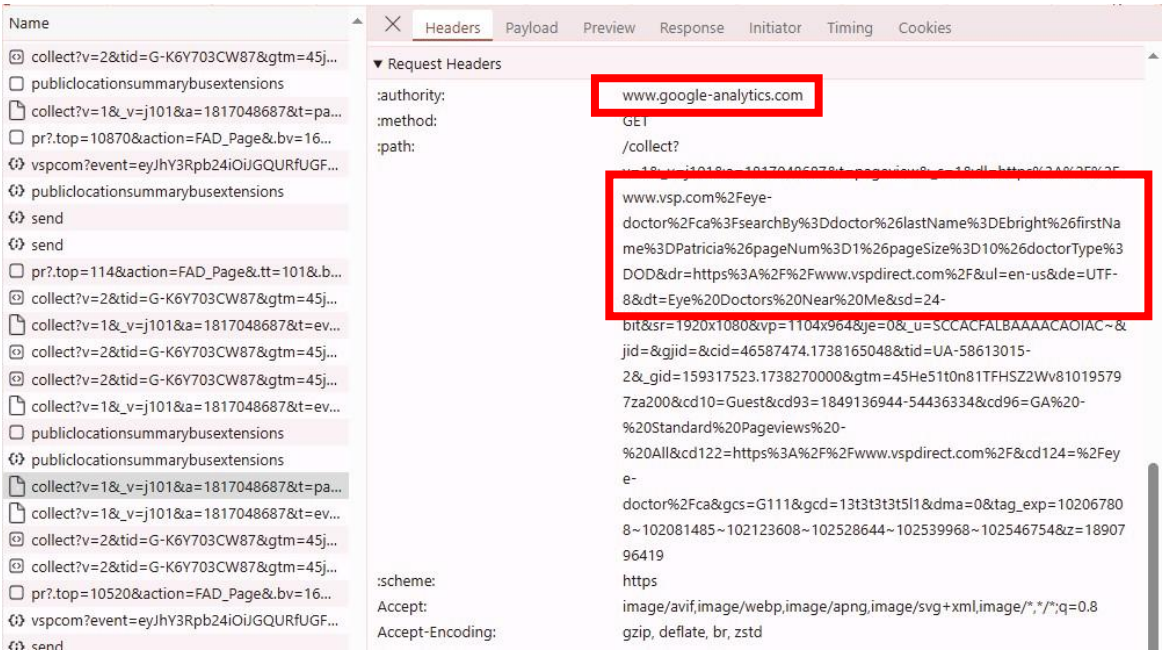
///

///



78. As shown above, the user typed "Ebright" into the "Last Name" text box, "Patricia" into the "First Name" text box, selected "Optometrist" as the "Doctor Type" using the drop-down menu, and selected "CA" using the "State" drop-down menu.

79. VSP transmitted all of this information to Google alongside its patients' personal identifiers.



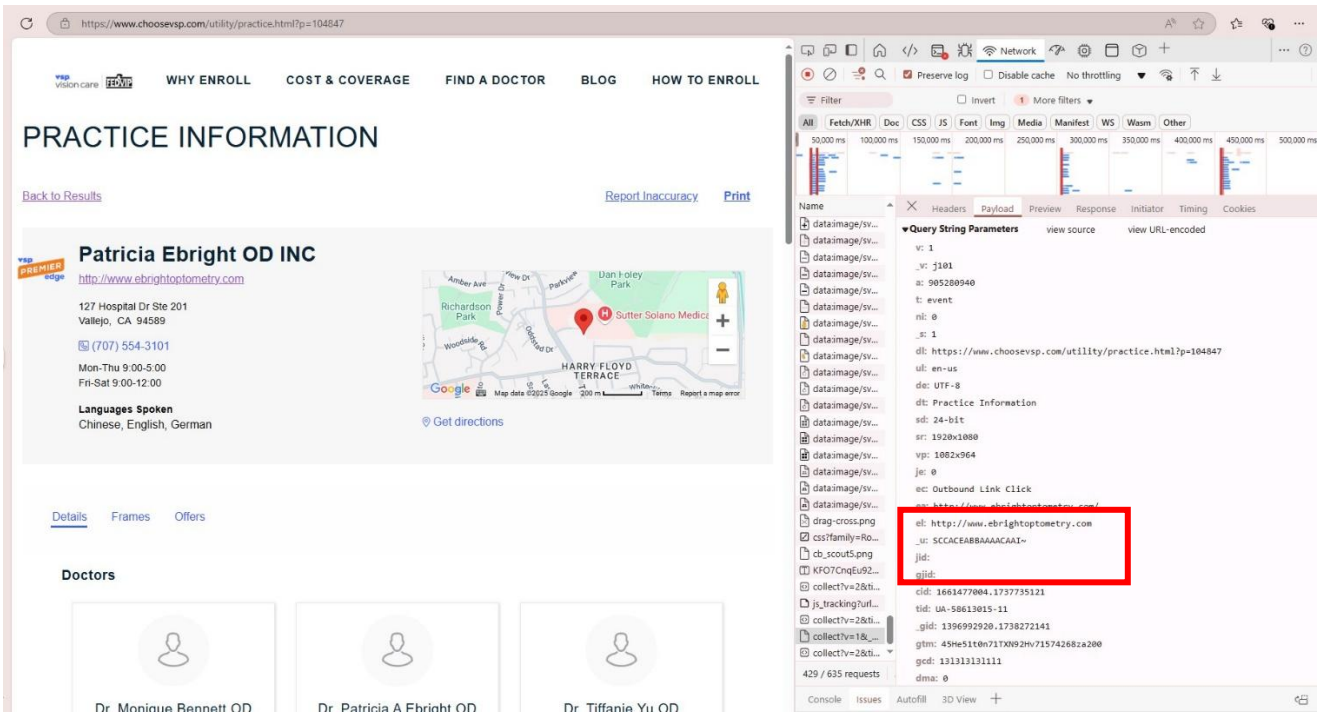
:authority:	www.google-analytics.com
:method:	GET
:path:	/collect? v=1&_v=j101&a=1817048687&t=pageview&_s=1&dl=https%3A%2F%2F www.vsp.com%2Feye- doctor%2Fca%3FsearchBy%3Ddoctor%26lastName%3DEbright%26firstNa me%3DPatricia%26pageNum%3D1%26pageSize%3D10%26doctorType%3 DOD&dr=https%3A%2F%2Fwww.vspdirect.com%2F&ul=en-us&de=UTF- 8&dt=Eye%20Doctors%20Near%20Me&sd=24- bit&sr=1920x1080&vp=1104x964&je=0&_u=SCCACFALBAAAACAOIAC~& jid=&gjid=&cid=46587474.1738165048&tid=UA-58613015- 2&_gid=159317523.1738270000&gtm=45He51t0n81TFHSZ2Wv81019579 7za200&cd10=Guest&cd93=1849136944-54436334&cd96=GA%20- %20Standard%20Pageviews%20- %20All&cd122=https%3A%2F%2Fwww.vspdirect.com%2F&cd124=%2Fey e- doctor%2Fca&gcs=G111&gcd=13t3t3t3t5l1&dma=0&tag_exp=10206780 8~102081485~102123608~102528644~102539968~102546754&z=18907 96419

Headers | Payload | Preview | Response | Initiator | Timing | Cookies

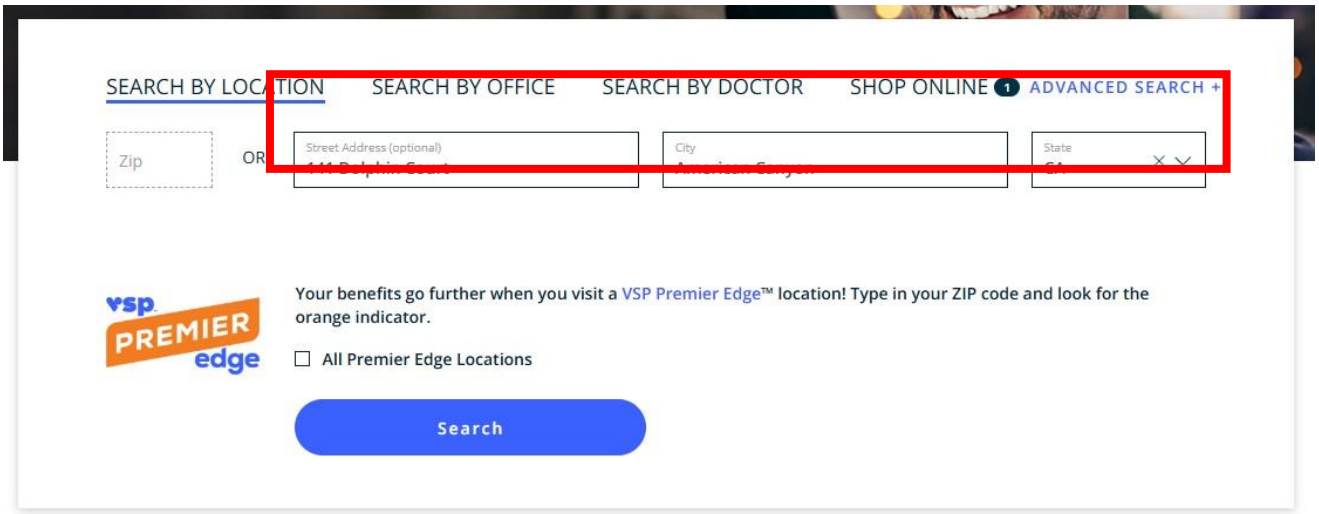
▼ **Query String Parameters** view source view URL-encoded

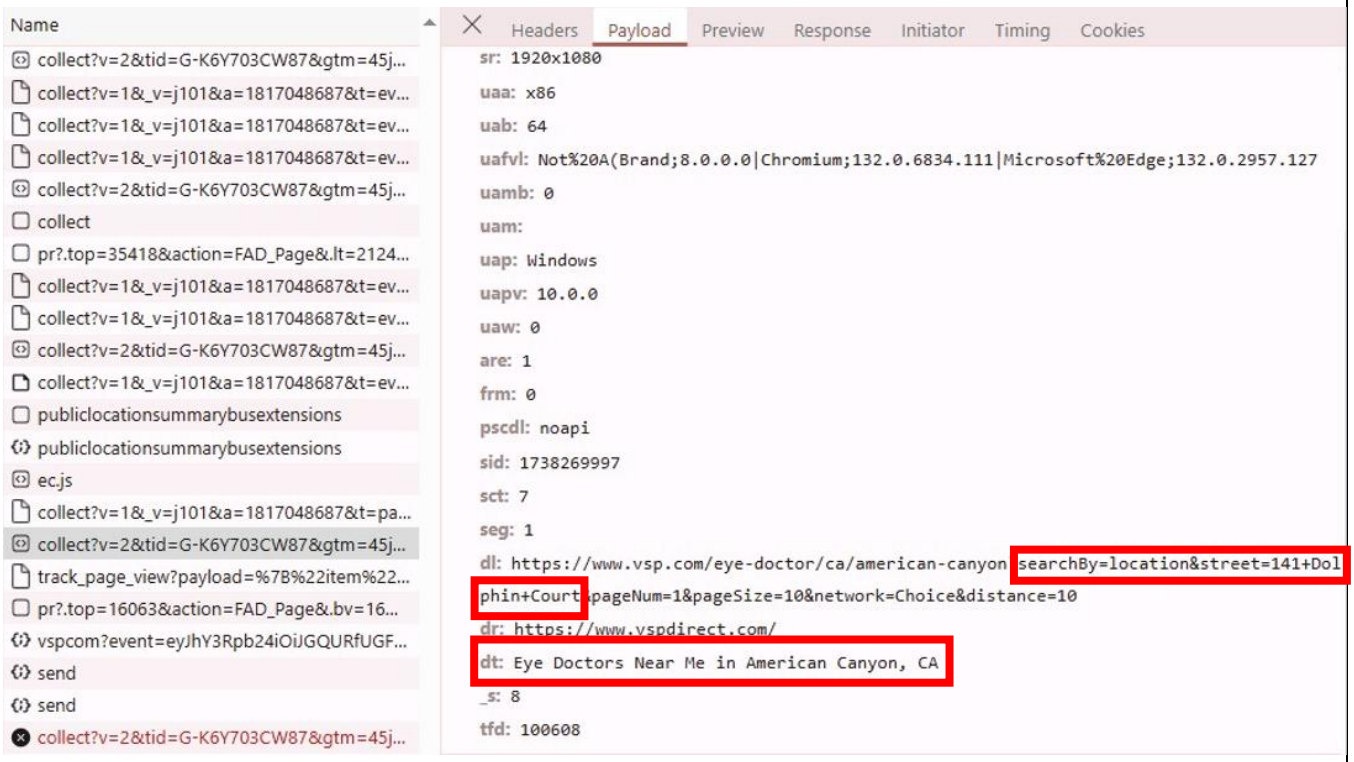
v: 1
_v: j101
a: 1817048687
t: pageview
_s: 1
dl: https://www.vsp.com/eye-doctor/ca?searchBy=doctor&lastName=Ebright&firstName=Patricia
&pageNum=1&pageSize=10&doctorType=OD
dr: https://www.vspdirect.com/
ul: en-us
de: UTF-8
dt: Eye Doctors Near Me

80. Additionally, when the user clicks on their physician's separate URL, that action is recorded as an "Outbound Link Click," which is transmitted to Google along with the specific URL and the users' device identifiers.


https://www.choosevsp.com/utility/practice.html?p=104847
WHY ENROLL
COST & COVERAGE
FIND A DOCTOR
BLOG
HOW TO ENROLL
PRACTICE INFORMATION
Back to Results
Report Inaccuracy
Print
Patricia Ebright OD INC
http://www.ebrightoptometry.com
127 Hospital Dr Ste 201
Vallejo, CA 94589
(707) 554-3101
Mon-Thu 9:00-5:00
Fri-Sat 9:00-12:00
Languages Spoken
Chinese, English, German
Get directions
Details
Frames
Offers
Doctors
Dr. Monique Bennett OD
Dr. Patricia A Ebright OD
Dr. Tiffanie Yu OD
Query String Parameters
view source
view URL-encoded
v: 1
_v: j101
a: 905280940
t: event
ni: 0
_s: 1
dl: https://www.choosevsp.com/utility/practice.html?p=104847
ul: en-us
de: UTF-8
dt: Practice Information
sd: 24-bit
sr: 1920x1080
vp: 1082x964
je: 0
ec: Outbound Link Click
el: http://www.ebrightoptometry.com
_u: SCCACEABBAAAACAAI~
jid:
gjid:
cid: 1661477004.1737735121
tid: UA-58613015-11
_gid: 1396992920.1738272141
gtm: 45He51t0n71TXN92Hv71574268za200
gcd: 13131313l111
dma: 0
429 / 635 requests

81. The user's street address is also communicated to Google when they use the "Search By Location" tool to identify a physician.



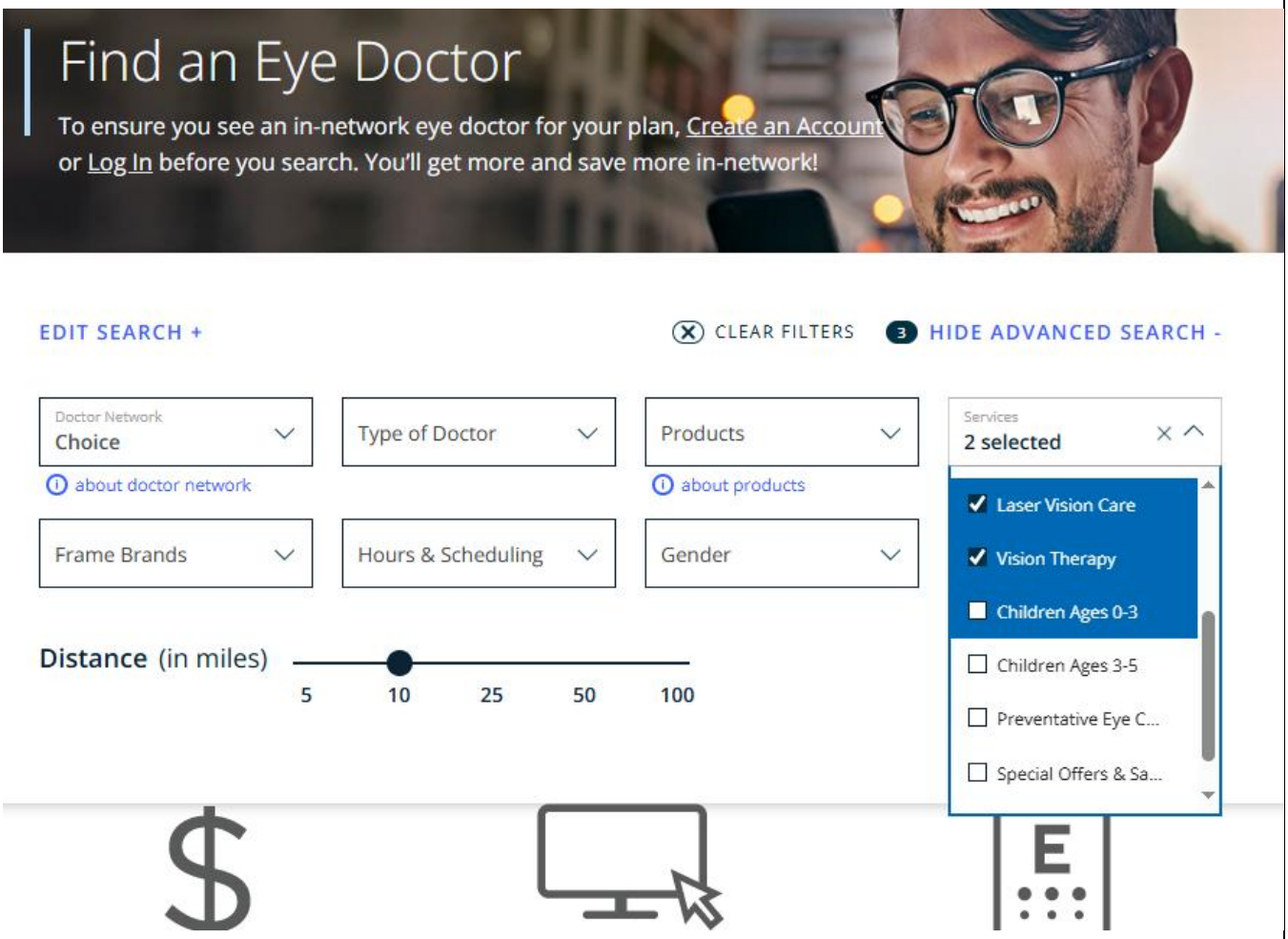


///

///

```
dl: https://www.vsp.com/eye-doctor/ca/american-canyon?searchBy=location&street=141+Dol
phin+Court&pageNum=1&pageSize=10&network=Choice&distance=10
dr: https://www.vspdirect.com/
dt: Eye Doctors Near Me in American Canyon, CA
_s: 8
```

82. Likewise, the "Advanced Search" filtering features also disseminate information that the user communicates via the "Services" drop-down tab. For example, if the same user selects that they are seeking "Vision Therapy," that information is recorded and disseminated to Google.



///

///

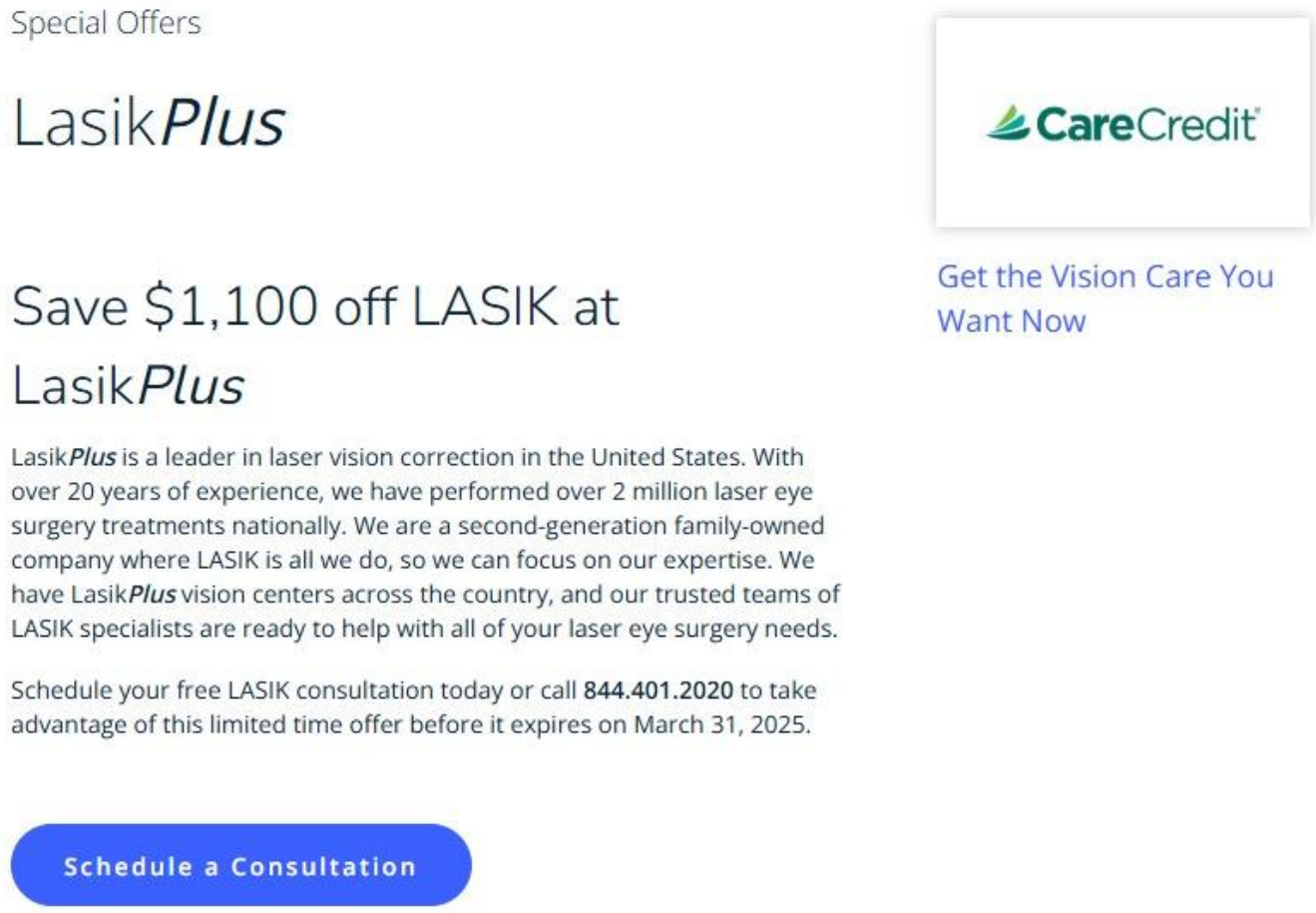
///

///

83. When the same user selects a specific procedure, such as "Laser Vision Care" or "Vision Therapy," that information is also received by Google alongside the user's IP address and other persistent identifiers.

84. Additionally, if the user schedules a consultation for specific treatments or special offers, that information is communicated without the user's knowledge or permission.

85. In the example below, the user clicked the "Schedule a Consultation" button.

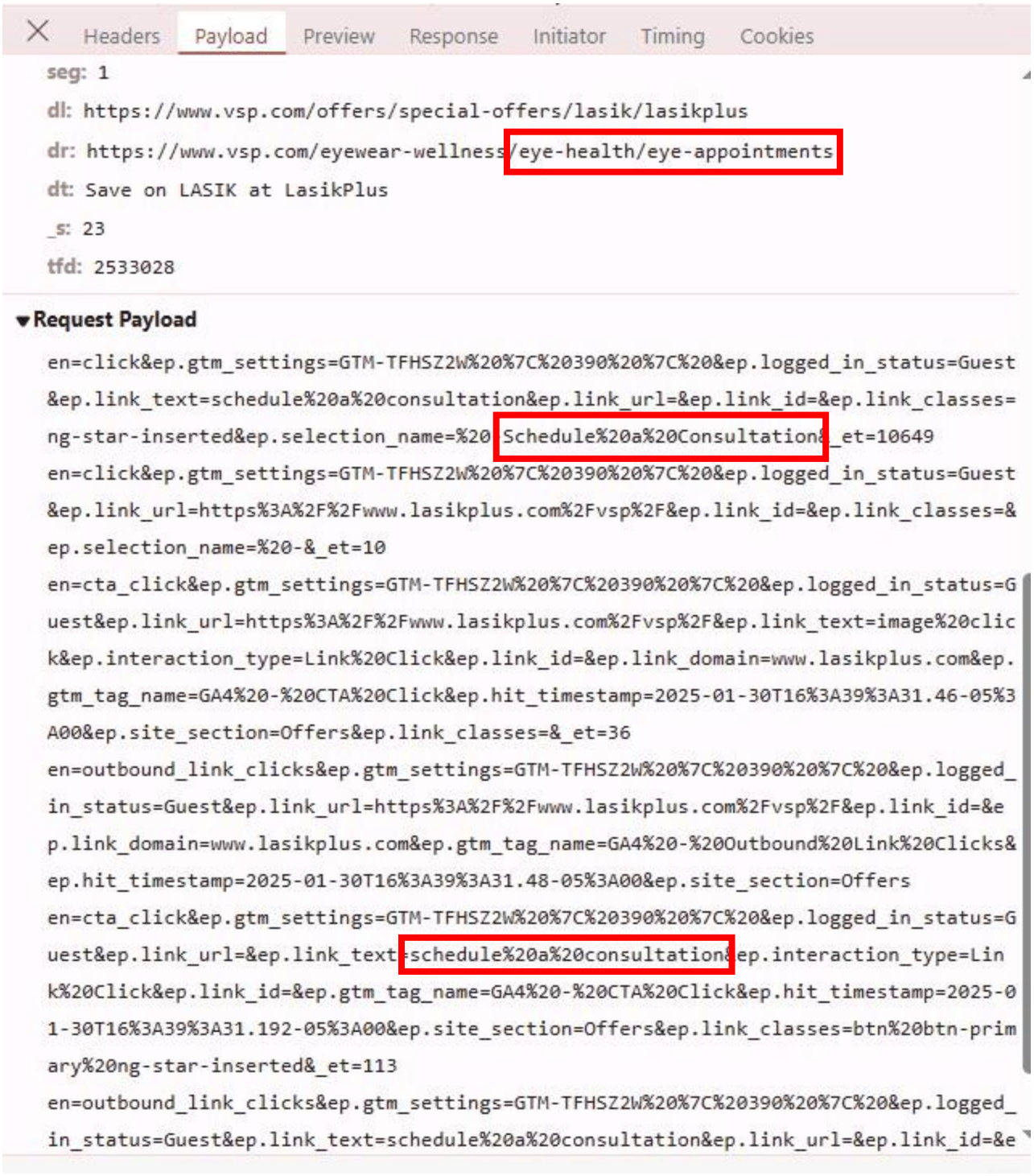


86. Upon doing so, their Private Information was sent to Google as shown in the image below.

///

///

///

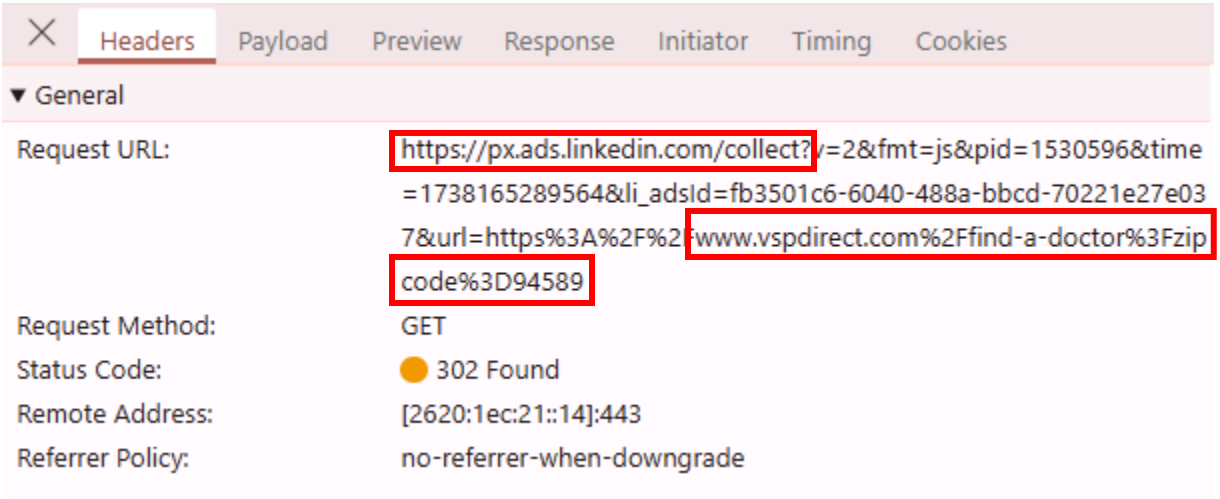


87. Like Meta, Google views, uses, and monetizes the data it receives for marketing and links Private Information to other information in its possession.

///

88. In addition, upon information and belief and as described above, Defendant has also installed LinkedIn's marketing tools and additional Tracking Tools on its servers and Web Properties to share patients' Private Information.

89. The image below shows that network traffic is sent to LinkedIn, which is now owned by Microsoft, for use in targeted advertising and training AI.



90. Like Meta, LinkedIn uses persistent identifiers to match a user to their real-world identity and any other information they have provided to LinkedIn, including but not limited to their email address, phone number, place of work, and additional demographic information. The image below shows a portion of the identifiers that VSP's Tracking Tools sent to LinkedIn.

///

///

///

///

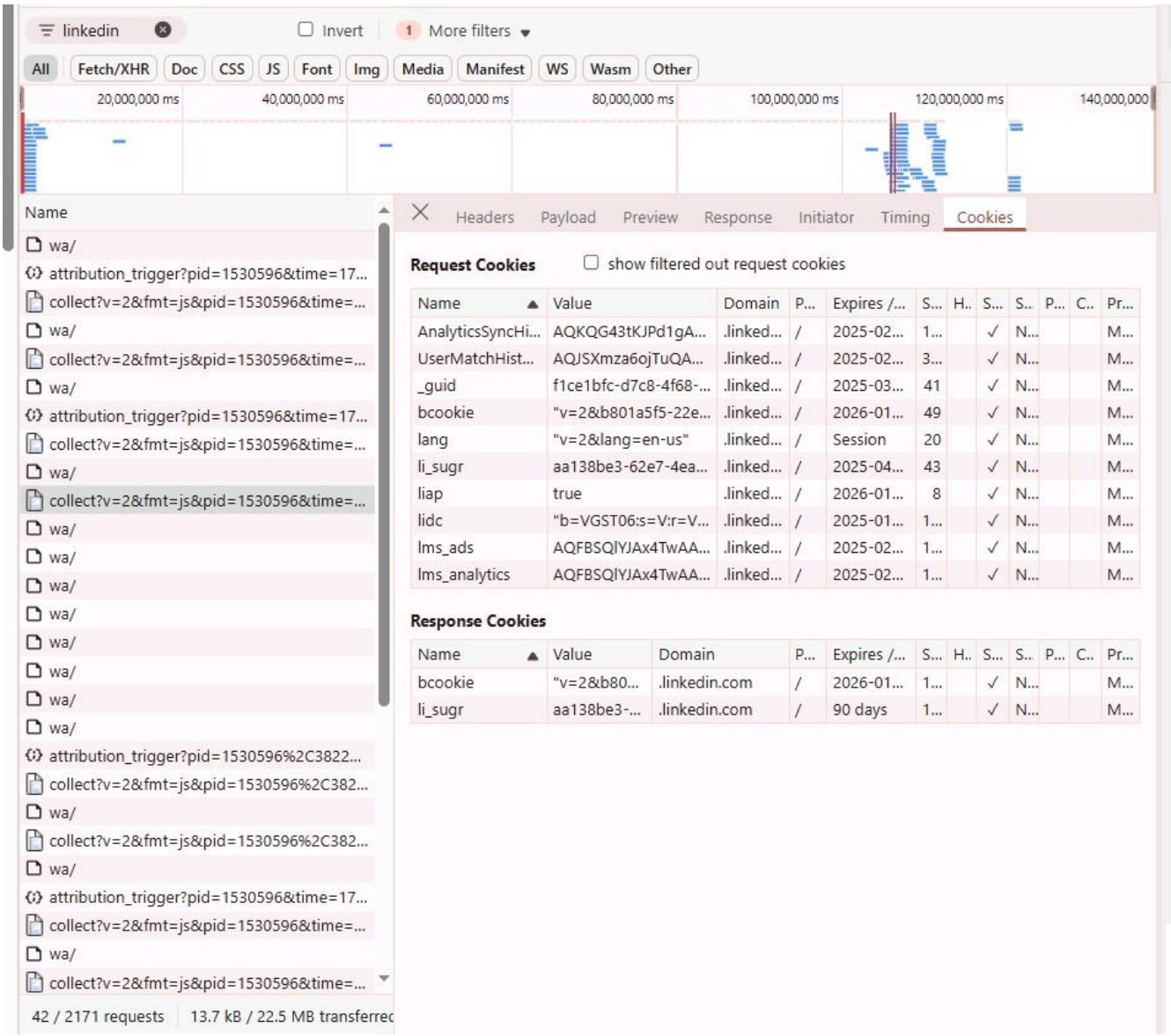
///

///

///

///

///



91. VSP did not disclose that the Tracking Technologies embedded in its Web Properties intercept, transmit, record, and disseminate Plaintiff's and Class Members' Private Information to Meta, Google, Microsoft, and additional third parties who use those companies' marketing services and/or scrape their Real Time Bidding systems to harvest sensitive Private Information.

92. Moreover, VSP never received consent or written authorization to disclose Plaintiff's and Class Members' Private Information in this manner.

///

D. Plaintiff's and Class Members' Private Information was Viewed and Used by Unauthorized Third Parties.

93. Unsurprisingly, the Tracking Technologies are not offered for "free" to companies like Defendant solely for Defendant's benefit. "Data is the new oil of the digital economy,"[15] and Meta has built its more-than $300 billion market capitalization on mining and using that 'digital' oil. Google, Microsoft, and other ad tech companies are similarly motivated, and Google's online advertising business generated 42.4% of global digital ad revenues in 2023.[16]

94. Thus, the large volumes of personal and sensitive health-related data Defendant divulged was actively viewed, examined, analyzed, curated, and used by Meta, Google, Microsoft, and others.

95. Tech companies acquire the raw data to transform it into a monetizable commodity, just as an oil company acquires crude oil to transform it into gasoline. Indeed, Meta and Google offer Tracking Tools free of charge,[17] and the price that Defendant paid was the data it allowed them to intercept from Plaintiff's and Class Members' devices, and the data that it disseminated directly from VSP's own servers.

96. Facebook is a "real identity platform,"[18] meaning users are allowed only one account and must share "the name they go by in everyday life."[19] To that end, when users must provide their first and last name, date of birth, and gender.[20]

///

[15] https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/ (last visited April 25, 2023).
[16] https://visiblealpha.com/blog/global-digital-advertising-revenues-a-look-at-the-big-three-alphabet-googl-meta-platforms-meta-amazon-com-amzn/ (last visited May 1, 2024).
[17] https://seodigitalgroup.com/facebook-pixel/ (last visited April 25, 2024).
[18] Sam Schechner and Jeff Horwitz, *How Many Users Does Facebook Have? The Company Struggles to Figure It Out*, WALL. ST. J. (Oct. 21, 2021).
[19] FACEBOOK, COMMUNITY STANDARDS, PART IV INTEGRITY AND AUTHENTICITY, https://www.facebook.com/communitystandards/integrity_authenticity (last visited April 5, 2023).
[20] FACEBOOK, SIGN UP, https://www.facebook.com/ (last visited April 25, 2023).

97. Meta sells advertising space by emphasizing its ability to target users,[21] and it is especially effective because it surveils user activity both on and off its own site (with the help of companies like Defendant).[22] This allows Meta to make inferences about users beyond what they explicitly disclose, and it compiles this information into a dataset called "Core Audiences," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.[23]

98. Advertisers can also build "Custom Audiences,"[24] which helps them reach "people who have already shown interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website."[25] With Custom Audiences, advertisers can target existing customers directly. They can also build "Lookalike Audiences," which "leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[26] Unlike Core Audiences, Custom Audiences and Lookalike Audiences are only available if the advertiser has sent its underlying data to Meta. This data can be supplied to Meta by manually

///

///

///

---

[21] FACEBOOK, WHY ADVERTISE ON FACEBOOK, https://www.facebook.com/business/help/205029060038706 (last visited April 25, 2023).

[22] FACEBOOK, ABOUT FACEBOOK PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited April 25, 2023).

[23] *Facebook, Easier, More Effective Ways to Reach the Right People on Facebook*, https://www.facebook.com/business/news/Core-Audiences (last visited April 25, 2023).

[24] *Facebook, About Custom Audiences*, https://www.facebook.com/business/help/744354708981227?id=2469097953376494 (last visited April 25, 2023).

[25] *Facebook, Ad Targeting, Help your ads Find the People Who Will Love Your Business*, https://www.facebook.com/business/ads/ad-targeting (last visited April 25, 2023).

[26] *Facebook, About Lookalike Audiences*, https://www.facebook.com/business/help/164749007013531?id=401668390442328 (last visited April 5, 2023).

uploading contact information for customers or by utilizing Meta's "Business Tools" like the Pixel and Conversions API.[27]

99. Meta does not merely collect information gathered by the Pixel and store it for safekeeping on its servers without ever viewing or accessing the information.

100. Instead, in accordance with the purpose of the Pixel, and to allow Meta to create Core, Custom, and Lookalike Audiences for advertising and marketing purposes, Meta viewed, processed, and analyzed Plaintiff's and Class Members' confidential Private Information. Upon information and belief, such viewing, processing, and analyzing was performed by computers and/or algorithms programmed and designed by Meta employees at the direction and behest of Meta.

101. Meta receives over 4 petabytes of information every day and uses software that views, categorizes, and extrapolates the data to augment human effort.[28] This process is known as "data ingestion" and allows "businesses to manage and make sense of large amounts of data."[29]

102. By using data ingestion tools, Meta can rapidly translate the information it receives from the Tracking Tools to display relevant ads to consumers. For example, if a consumer visits a retailer's webpage and places an item in their shopping cart without purchasing it, the next time the shopper visits

---

[27] *Facebook, Create a Customer List Custom Audience*, https://www.facebook.com/business/help/170456843145568?id=2469097953376494 (last visited April 5, 2023); *Facebook, Create a Website Custom Audience*, https://www.facebook.com/business/help/1474662202748341?id=2469097953376494 (last visited April 5, 2023).

[28] https://medium.com/@srank2000/how-facebook-handles-the-4-petabyte-of-data-generated-per-day-ab86877956f4. Facebook employees would not be able to view each piece of data individually – millions of them per second – without the aid of technology. Just as a microscope or telescope allows the user to see very small or very distant objects by zooming in, however, Facebook's big data management software allows the company to see all this data at once by zooming out.

[29] https://scaleyourapp.com/what-database-does-facebook-use-a-1000-feet-deep-dive/. Facebook uses ODS, Scuba, and Hive to manage its massive data stores. These technologies are not traditional databases; they are specialized databases for big data designed to process data specifically for analysis—"such as [viewing] hidden patterns, correlations, market trends and customer preferences."

Facebook or Instagram, an ad for that item will appear on the shopper's Facebook page or Instagram account.[30] This evidences the fact that Meta views and categorizes data as it is received from the Pixel.

103. Moreover, even if Meta eventually deletes or anonymizes sensitive information that it receives, it must first view that information to identify it as containing sensitive information suitable for removal. Accordingly, there is a breach of confidentiality the instant the information is disclosed or received without authorization. As described by the HHS Bulletin:

> It is insufficient for a tracking technology vendor to agree to remove PHI from the information it receives or de-identify the PHI before the vendor saves the information. Any disclosure of PHI to the vendor without individuals' authorizations requires the vendor to have a signed BAA in place **and** requires that there is an applicable Privacy Rule permission for disclosure.

(emphasis in original).

E. Defendant Was Enriched and Benefitted from the Use of the Tracking Technology and Private Information Had Financial Value

104. The Tracking Technologies served the sole purpose of bolstering Defendant's profits via marketing and advertising.

105. In exchange for bartering away and disclosing the Private Information of its patients and customers, VSP is compensated by Meta, Google, Microsoft, and the like in the form of enhanced advertising services and more cost-efficient marketing.

106. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions. Upon information and belief, as part of its marketing campaign, VSP re-targeted patients and potential patients.

///

///

[30] *A Complete Guide to Facebook Tracking for Beginners*, OBERLO, Oct. 5, 2021, https://www.oberlo.com/blog/facebook-pixel.

107. By utilizing the Tracking Technologies, the cost of advertising and retargeting was reduced, thereby benefitting Defendant.

108. VSP's disclosure of Private Information harmed Plaintiff and the Class. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is expected to continue to increase, and estimates for 2022 were as high as $434 per user, constituting over $200 billion industry wide.

109. The value of health data in particular is well-known. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry" in which it described the extensive market for health data, observing that the market for this data is both lucrative and a significant risk to privacy.[31]

110. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[32] Accordingly, patient data that can be linked to a specific individual is even more valuable.

111. There is also a market for data in which consumers can participate. Personal information has been recognized by courts as extremely valuable. *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

///

///

[31] *See* https://time.com/4588104/medical-data-industry/ (last visited April 25, 2023).

[32] *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited April 25, 2023).

112. Several companies have products through which they pay consumers for a license to track their data. Google, Nielsen, UpVoice, HoneyGain, and SavvyConnect are all companies that pay for browsing historical information.

113. Meta also has paid users for their digital information, including browsing history. Until 2019, Meta ran a "Facebook Research" app through which it paid $20 a month for a license to collect browsing history information and other communications from consumers between the ages 13 and 35.

114. Additionally, healthcare data is extremely valuable to bad actors. Health care records may be valued at up to $250 per record on the black market.[33]

115. Personal information has private value beyond its use as a bare commodity.[34] The value of personal information is thus inherently related to the value of privacy, which is a question that has been researched in multiple fields including decision science, economics, information systems, management, health care, and marketing.[35] This research has approached the valuation of personal information from multiple perspectives:[36]

(a) The amount one would accept to relinquish their data;

(b) The amount one would spend to protect their data;

(c) The potential harm from data exposure; and

(d) The benefit a data holder could gain from acquiring data.

116. These approaches can be used to establish a set of data points for the reasonable estimation of the value of personal information and non-public medical information such as patient status.

[33] Tori Taylor, *Hackers, Breaches, and the Value of Healthcare Data, SecureLink* (June 30, 2021), https://www.securelink.com/blog/healthcare-data-new-prize-hackers.

[34] Wagner, et. al (2018); Acquisti, Alessandro, Curtis Taylor, and Liad Wagman (2016); Li, Xiao-Bai, Xiaoping Liu, and Luvai Motiwalla (2021).

[35] Fehrenbach David, Carolina Herrando. "The effect of customer-perceived value when paying for a product with personal data: A real-life experimental study." *Journal of Business Research* 137 (2021): 222-232; Li, Xiao-Bai, Xiaoping Liu, and Luvai Motiwalla (2021); Alorwu, et al. (2024).

[36] Acquisti, Alessandro, Curtis Taylor, and Liad Wagman (2016).

117. In addition, numerous services exist that charge fees to monitor and remove personal information from data brokers and search databases. For example, Privacy Bee charges $197 per year.[37] Other similar services exist today, such as DeleteMe®, which removes information from all major data broker websites for $129 per year,[38] deleteme™ which charges one-time fees ranging from $100 to $500 for search engine and data breach removals,[39] Incogni.com which charges $179 per year to remove information from major data broker websites and search databases,[40] and ReputationDefender, a service that charges $99 per year to remove personal information from various databases.[41] These provide a baseline market valuation of personal information

F. Defendant Violated HIPAA and Industry Standards.

118. In December 2022, HHS issued a bulletin (the "HHS Bulletin") warning regulated entities like Defendant about the risks presented by the use of Tracking Tools on their websites:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.***[42]

119. In other words, the HHS has expressly stated that entities who implement Tracking Tools, such as Defendant, have violated HIPAA Rules unless they have obtained a HIPAA-complaint authorization from their patients.

---

[37] Privacy Bee - Pricing, privacybee.com, accessed September 26, 2024.
[38] Privacy Protection Plans - JoinDeleteMe, joindeleteme.com, accessed September 26, 2024.
[39] Deleteme - Services Pricing, deleteme.com, accessed September 26, 2024.
[40] Incogni – About Us, incogni.com, accessed September 26, 2024.
[41] ReputationDefender signup, me.reputationdefender.com, accessed September 26, 2024. ReputationDefender was previously known as Reputation.com and has been offering this service since at least 2012. Also see: https://www.nytimes.com/2012/12/09/business/company-envisions-vaults-for-personal-data.html
[42] *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited October 11, 2023) (emphasis added).

120. The HHS Bulletin further warns that:

> While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, ***because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.*** [43]

121. In addition, HHS and the FTC have recently issued a letter, once again admonishing entities like Defendant to stop using Tracking Tools:

> If you are a covered entity or business associate ("regulated entities") under HIPAA, you must comply with the HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules), with regard to protected health information (PHI) that is transmitted or maintained in electronic or any other form or medium. ***The HIPAA Rules apply when the information that a regulated entity collects through tracking technologies or discloses to third parties (e.g., tracking technology vendors) includes PHI. . .*** Even if you are not covered by HIPAA, you still have an obligation to protect against impermissible disclosures of personal health information under the FTC Act and the FTC Health Breach Notification Rule. . . As recent FTC enforcement actions demonstrate, it is essential to monitor data flows of health information to third parties via technologies you have integrated into your website or app. The disclosure of such information without a consumer's authorization can, in some circumstances, violate the FTC Act as well as constitute a breach of security under the FTC's Health Breach Notification Rule.[44]

122. Under Federal Law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[45]

123. The HIPAA Privacy Rule, located at 45 CFR Part 160 and Subparts A and E of Part 164, "establishes national standards to protect individuals' medical records and other individually identifiable

///

---

[43] *Id.*

[44] *Re: Use of Online Tracking Technologies*, U.S. Dept. of Health & Hum. Servs. and Fed. Trade. Comm'n (July 20, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf.

[45] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

health information (collectively defined as 'protected health information') and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically."[46]

124. The Privacy Rule broadly defines "protected health information" ("PHI") as individually identifiable health information ("IIHI") that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium." 45 C.F.R. § 160.103.

125. IIHI is defined as "a subset of health information, including demographic information collected from an individual" that is: (1) "created or received by a health care provider, health plan, employer, or health care clearinghouse"; (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual"; and (3) either (a) "identifies the individual" or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

126. Under the HIPAA de-identification rule, "health information is not individually identifiable only if": (1) an expert "determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information" and "documents the methods and results of the analysis that justify such determination'"; or (2) "the following identifiers of the individual or of relatives, employers, or household members of the individual are removed;

(a) Names;
***
(b) Medical record numbers;
***

[46] HHS.gov, HIPAA For Professionals (last visited October 12, 2023), https://www.hhs.gov/hipaa/forprofessionals/privacy/index.html.

> (c) Account numbers;
> ***
> (d) Device identifiers and serial numbers;
>
> (e) Web Universal Resource Locators (URLs);
>
> (f) Internet Protocol (IP) address numbers; … and
>
> (g) Any other unique identifying number, characteristic, or code…; and" The covered entity must not "have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information."
> 45 C.F.R. § 160.514.

127. The HIPAA Privacy Rule requires any "covered entity"—which includes pharmacies—to maintain appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of protected health information without authorization. 45 C.F.R. §§ 160.103, 164.502.

128. An individual or corporation violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-1320d-9 ("Part C"): "(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual." The statute states that a "person … shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained by a covered entity … and the individual obtained or disclosed such information without authorization." 42 U.S.C. § 1320d-6.

129. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to Defendant when it is knowingly disclosing individually identifiable health information relating to an individual, as those terms are defined under HIPAA.

130. Violation of 42 U.S.C. § 1320d-6 is subject to criminal penalties. 42 U.S.C. § 1320d-6(b). There is a penalty enhancement where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm."

In such cases, the entity that knowingly obtains individually identifiable health information relating to an individual shall "be fined not more than $250,000, imprisoned not more than 10 years, or both."

131. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the HHS instructs:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data… If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[47]

132. In its guidance for Marketing, the HHS further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list*. (Emphasis added).[48]

133. As alleged above, there is an HHS Bulletin that highlights the obligations of "regulated entities," which are HIPAA-covered entities and business associates, when using tracking technologies.[49]

134. The Bulletin expressly provides that "[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."

---

[47] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last visited October 11, 2023).

[48] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf (last visited Oct. 12, 2023).

[49] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

135. Defendant's actions violated HIPAA Rules.

G. IP Addresses, Mobile Advertising IDs, and Other Devices Identifiers Constitute Personally Identifiable Information.

136. VSP also disclosed and otherwise assisted third parties with intercepting Plaintiff's and Class Members' IP addresses, Mobile Advertising IDs, and other device identifiers that are uniquely linked to specific individuals.

137. An IP address is a number that identifies the address of a device connected to the Internet, and it is used to identify and route communications on the Internet.

138. Internet service providers, websites, and third-party tracking companies use individual's IP addresses to facilitate and track Internet communications.

139. Meta tracks every IP address ever associated with a Facebook user and uses IP addresses to target individual homes and their occupants with advertising. In addition, as noted above, Defendant used Google Analytics tools, Google Tag Manager, and DoubleClick tracking tools without anonymizing users' IP addresses.

140. Under HIPAA, an IP address is considered personally identifiable information:

- HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. See 45 C.F.R. § 164.514 (2).
- HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); See also, 45 C.F.R. § 164.514(b)(2)(i)(O).

141. Consequently, by disclosing IP addresses, Defendant's business practices violated HIPAA and industry privacy standards.

///

142. Likewise, on information and belief, the Tracking Tools used by Defendant also transmitted users' Mobile Advertising IDs ("MAID") and may have transmitted AAID (Android Advertising ID), Router SSID, Hardware ID, IMEI (International Mobile Equipment Identity), and other persistent identifiers.

143. According to the FTC, "MAIDs and other persistent identifiers, by design, enable direct communication with individual consumers, are used to amass profiles of individuals over time and across different web and mobile services, and are the basis to make decisions and insights about individual consumers."[50]

G. Plaintiff Brian Tash's Experience with Defendant's Web Properties

144. Plaintiff Brian Tash is a vision patient that has been insured by VSP and used VSP's services for more than 20 years.

145. As a patient, and in order to obtain medical treatment and insurance services, Plaintiff Tash accessed and used VSP's Web Properties on his phone and computer.

146. For approximately the last decade, he has used these same devices to access his Facebook account, email, and LinkedIn account and stays logged into these accounts.

147. Plaintiff Tash communicated his Private Information to VSP when he used the Web Properties, and he specifically recalls using the "Find a Doctor" form and webpage to identify an in-network healthcare provider in or around 2021 following a recent move.

148. More specifically, he recalls using every filtering feature available to obtain the narrowest selection, which communicated the following: (1) the type of physician or medical provider he was

///

[50] *See In the Matter of Gravy Analytics, Inc., a corporation, and Venntel, Inc., a corporation* (Compl. 212-3025), available online at https://www.ftc.gov/system/files/ftc_gov/pdf/2123035gravyanalyticscomplaint.pdf (last accessed Jan. 4, 2025).

seeking; (2) the specific medical services he was seeking; (3) the vision products sought during his visit; (4) his location; and (5) additional details about his desired physician and their practice area.

149. Upon entering his Private Information and clicking the "Search" button, his search parameters and the contents of his communications were sent to Meta, Google, and LinkedIn alongside his Facebook ID, IP address, and additional persistent identifiers that reveal his real-world identity.

150. Plaintiff Tash reasonably expected that—as a patient seeking medical treatment—his communications were confidential and would not be received by Meta, Google, LinkedIn, and other unknown third-parties, or used for marketing purposes, without his express written consent. That was not the case.

* * *

151. The risk to Plaintiff's and other patients' privacy is ongoing in nature because the Private Information Meta, Google, LinkedIn, and other third parties received can be used for years to come.

152. In fact, many companies are using data obtained by Tracking Tools to decide whether to raise insurance premiums or deny coverage.[51]

153. Through the process detailed in this Complaint, VSP unlawfully assisted third parties with intercepting Plaintiff's communications and health information via the Pixel and Google Analytics, further divulged that information via Conversions API and other server-to-server Tracking Tools, breached confidentiality, violated Plaintiff's right to privacy, and unlawfully disclosed their personally identifiable information and protected health information.

///

[51] *See In re Consumer Vehicle Driving Data Tracking Litig*., 737 F. Supp. 3d 1355 (U.S. Jud. Pan. Mult. Lit. 2024)(alleging General Motors and OnStar improperly used Tracking Tools to disseminate information to third-parties); *see also The State of Texas v. The Allstate Corporation et al., Dist. Ct. of Tex*., Montgomery Cty. (available online at https://www.texasattorneygeneral.gov/sites/default/files/images/press/Allstate%20and%20Arity%20Petition%20Filed.pdf).

154. Plaintiff was unaware that VSP installed Tracking Tools on its Web Properties because, amongst other things, the Tracking Tools were and are completely invisible, and Plaintiff reasonably believed that his insurance provider, which also owns several eye care clinics and is actively acquiring additional practices, would safeguard his privacy in compliance with industry standards, HIPAA, and relevant laws.

155. Plaintiff has a continuing interest in ensuring that future communications with Defendant are protected and safeguarded from future unauthorized disclosure and to know the precise categories of information disclosed, to whom it was disclosed, and why it was disclosed.

TOLLING

156. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiff did not know (and had no way of knowing) that his Private Information was intercepted and unlawfully disclosed to Meta, Google, Microsoft, or any other third-parties in the manner described herein because: (1) Defendant kept this information secret, (2) the Tracking Tools were invisible when Plaintiff and Class Members used the Web Properties; and (3) a portion of the Tracking Tools cause direct communications between Defendant's servers and third party servers that Plaintiff has no access to whatsoever.

CLASS ACTION ALLEGATIONS

157. **Class Definition:** Plaintiff brings this action on behalf of himself and other similarly situated individuals defined as follows:

> **Nationwide Class:** United States citizens who, during the class period, used Defendant's Web Properties and had their personally identifiable information or protected health information disclosed to Meta, Google, or Microsoft as a result of using the Web Properties.

> **California Class:** All California residents who, during the Class Period, used Defendant's Web Properties and had their personally identifiable information or protected health information disclosed to Meta, Google, or Microsoft as a result of using the Web Properties.

158. Plaintiff reserves the right to modify the class definitions or add sub-classes as needed prior to filing a motion for class certification.

159. The "Class Period" is the period beginning on the date established by the Court's determination of any applicable statute of limitations, after consideration of any tolling, concealment, and accrual issues, and ending on the date of entry of judgement or preliminary approval of a settlement.

160. Excluded from the Class are Defendant; any affiliate, parent, or subsidiary of Defendant; any entity in which Defendant has a controlling interest; any officer director, or employee of Defendant; any successor or assign of Defendant; anyone employed by counsel in this action; any judge to whom this case is assigned, his or her spouse and immediate family members; and members of the judge's staff.

161. Numerosity/Ascertainability. Members of the Class are so numerous that joinder of all members would be unfeasible and not practicable. The exact number of Class Members is unknown to Plaintiff currently. However, it is estimated that there are thousands of individuals in the Class. The identity of such membership is readily ascertainable from Defendant's records and non-party Meta's records.

162. Typicality. Plaintiff's claims are typical of the claims of the Class because Plaintiff used Defendant's Web Properties and had their personally identifiable information and protected health information disclosed to third parties such as Facebook and Google without their express written authorization or knowledge. Plaintiff's claims are based on the same legal theories as the claims of other Class Members.

163. Adequacy. Plaintiff is fully prepared to take all necessary steps to represent fairly and adequately the interests of the Class Members. Plaintiff's interests are coincident with, and not

antagonistic to, those of the Class Members. Plaintiff is represented by attorneys with experience in the prosecution of class action litigation generally and in the emerging field of digital privacy litigation specifically. Plaintiff's attorneys are committed to vigorously prosecuting this action on behalf of the Class Members.

164. Common Questions of Law and Fact Predominate/Well Defined Community of Interest. Questions of law and fact common to the Class Members predominate over questions that may affect only individual Class Members because Defendant has acted on grounds generally applicable to the Class. Such generally applicable conduct is inherent in Defendant's wrongful conduct. The following questions of law and fact are common to the Class:

(a) Whether VSP intentionally tapped the lines of internet communication between patients and their medical providers;

(b) Whether the Web Properties surreptitiously track PII, PHI, and related communications and simultaneously disclose(d) that information to Meta, Google, and/or other third parties;

(c) Whether Meta and/or Google is a third-party eavesdropper;

(d) Whether VSP's disclosures of PII, PHI, and related communications constitute an affirmative act of communication;

(e) Whether VSP's conduct, which allowed third parties to view Plaintiff's and Class Members' PII and PHI, resulted in a breach of confidentiality;

(f) Whether VSP's conduct, which allowed third parties to view Plaintiff's and Class Members' PII and PHI, resulted in a breach of confidence;

(g) Whether VSP violated Plaintiff's and Class Members' privacy rights by using Tracking Technologies to communicate patients' Private Information to third parties;

///

///

(h) Whether Plaintiff and Class Members are entitled to damages under CIPA, the CMIA, or any other relevant statute;

(i) Whether VSP's actions violated the Unfair Competition Law;

(j) Whether VSP's actions violated Plaintiff's and Class Members' privacy rights as provided by the California Constitution;

(k) Whether VSP violates HIPAA by requiring patients to affirmatively opt-out of having their information shared for marketing purposes;

165. Superiority. Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit many similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons a method for obtaining redress on claims that could not practicably be pursued individually, substantially outweighs potential difficulties in management of this class action. Plaintiff is unaware of any special difficulty to be encountered in litigating this action that would preclude its maintenance as a class action.

CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION
Violation Of the California Invasion of Privacy Act,
Cal. Penal Code § 631, *et seq.*
(On Behalf of Plaintiff and the California Class)

166. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the proposed Class.

167. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630 to 638. The Act begins with its statement of purpose.

> The Legislature thereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping

> upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

Cal. Penal Code § 630.

168. California Penal Code § 631(a) provides, in pertinent part (emphasis added):

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner … willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or **who aids, agrees with, employs, or conspires** with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars ($2,500).

169. Under CIPA, VSP must show it had the consent of all parties to a communication.

170. At all relevant times, VSP aided, employed, agreed with, and conspired with third parties, including Meta and Google, to track and intercept Plaintiff's and Class Members' internet communications. These communications were transmitted to and intercepted by a third party during the communication and without the knowledge, authorization, or consent of Plaintiff and Class Members.

171. VSP intentionally inserted an electronic listening device onto Plaintiff's and Class Members' web browsers and devices that, without their knowledge and consent, tracked and transmitted the substance of their confidential communications to Meta, Google, and other unauthorized third parties—each of whom constitute a "person" within the meaning of the statute.

172. VSP willingly facilitated the interception and collection of Plaintiff's and Class Members' Private Information by embedding the Meta Pixel on its Web Properties.

///

///

173. Moreover, unlike past Meta business tools such as the Facebook Like Button and older web beacons, the Meta Pixel, Conversion API, Google Tag Manager, Google Analytics, and tracking SDKs are: (1) completely invisible to website and app users; and (2) VSP has full control over these tools, including where they are embedded, what information is tracked and transmitted, and how events are categorized prior to their transmission.

174. VSP's Tracking Technologies constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, they fall under the broad catch-all category of "any other manner."

175. VSP failed to disclose its use of the Tracking Technologies to specifically track and automatically and simultaneously transmit Plaintiff's and Class Members' communications to Meta, Google, LinkedIn, and other undisclosed third-parties.

176. A portion of the Tracking Technologies—such as the Meta Pixel, Google Analytics, and Google Tag Manager—are designed to transmit a website user's actions and communications contemporaneously as the user initiates each communication. As a result, the user's communications are intercepted in transit to the intended recipient—VSP—before reaching VSP's server.[52]

177. VSP violated CIPA by aiding and permitting third parties to intercept and receive its patients' online communications in real time as they were made. Importantly, Meta, Google, and other unauthorized third parties would not have intercepted or received the contents of these communications but for VSP's actions, including its decision to install the Tracking Tools on its Web Properties.

178. By disclosing Plaintiff's and Class Members' Private Information, VSP violated Plaintiff's and Class Members statutorily protected right to privacy.

179. As a result of the above violations, and pursuant to CIPA Section 637.2, VSP is liable to Plaintiff and Class Members for treble actual damages related to their loss of privacy in an amount to be

[52] VSP's use of Conversions API and similar server-side Tracking Tools resulted in the divulgence, as opposed to the interception, of Plaintiff's communications.

determined at trial or for statutory damages in the amount of $5,000 per violation. Section 637.2 specifically states that "[it] is not a necessary prerequisite to an action pursuant to this section that the Plaintiffs have suffered, or be threatened with, actual damages."

180. Under the statute, VSP is also liable for reasonable attorney's fees, litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by the Defendant in the future.

SECOND CAUSE OF ACTION
Violation of the California Invasion of Privacy Act,
Cal. Penal Code § 638.51(a)

181. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

182. CIPA § 638.51(a) proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

183. A "pen register" is a "device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of the communication." Cal. Penal Code § 638.50(b).

184. The Tracking Tools are "pen registers" because they are device[s] or process[es]" that "capture[d]" the "routing, addressing, or signaling information" from Plaintiff and Class Members' electronic communications. *Id.*

185. At all relevant times, VSP installed the Tracking Tools—which are pen registers—onto Plaintiff's and Class Members' browsers, and it used the Tracking Tools to collect Plaintiff's and Class Members' Private Information.

186. Plaintiff and Class Members did not provide their consent to VSP's installation or use of the Tracking Tools.

187. VSP did not obtain a court order to install or use the Tracking Tools.

188. Pursuant to Cal. Penal Code § 637.2, Plaintiff and Class Members have been injured by VSP's violations of CIPA § 638.51(a), and each seek statutory damages of $5,000 for each of VSP's violations of CIPA § 638.51(a).

THIRD CAUSE OF ACTION
Violation Of the California Confidentiality of Medical Information Act
Cal. Civ. Code § 56, *et seq.*
(On Behalf of Plaintiff and the California Class)

189. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

190. The California Confidentiality of Medical Information Act, Cal. Civ. Code § 56, *et seq* ("CMIA") prohibits health care providers from disclosing medical information relating to their patients without a patient's express authorization. Medical information refers to "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care… regarding a patient's medical history, mental or physical condition, or treatment." 'Individually Identifiable' means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual..." Cal. Civ. Code § 56.05.

191. Defendant is a healthcare provider as defined by Cal. Civ. Code § 56.06.

192. Plaintiff and Class Members are patients of VSP and, as health care providers, VSP has an ongoing obligation to comply with the CMIA's requirements with respect to Plaintiff's and Class Members' confidential medical information.

193. As set forth above, names, addresses, telephone numbers, email addresses, device identifiers, web URLs, IP addresses, and other characteristics that can uniquely identify Plaintiff and Class Members are transmitted to Meta and Google in combination with insurance information, medical

///

conditions, medical concerns, treatment(s) sought by the patients, and other patient searches and queries. This PHI and PII constitutes confidential information under the CMIA.

194. The Facebook ID is also an identifier that allows identification of a particular individual. Along with patients' confidential Private Information, VSP disclosed its patients' Facebook IDs.

195. Pursuant to the CMIA, the information communicated to VSP and disclosed to Meta, Google, and other third parties constitutes medical information because it is patient information derived from a health care provider regarding a patient's medical treatment and physical condition and is received in combination with individually identifying information. Cal. Civ. Code § 56.05(i).

196. As set forth above, Facebook views, processes, and analyzes the confidential medical information it receives via the Facebook Tracking Pixel, Conversions API, SDKs, and other Facebook business tools. Facebook then uses the viewed confidential information to create Audiences for advertising and marketing purposes.

197. Similarly, Google also views, processes, and analyzes the confidential medical information it receives via Google Analytics. Google then uses the viewed confidential information for advertising and marketing purposes.

198. Defendant failed to obtain Plaintiff's and Class Members' authorization for the disclosure of medical information.

199. Pursuant to CMIA Section 56.11, a valid authorization for disclosure of medical information must: (1) be "clearly separate from any other language present on the same page and … executed by a signature which serves no other purpose than to execute the authorization;" (2) be signed and dated by the patient or their representative; (3) state the name and function of the third party that receives the information; and (4) state a specific date after which the authorization expires. The information set forth on VSP's Web Properties, including the website's Privacy Policy and Notice of

Privacy Practices, does not qualify as a valid disclosure or authorization.

200. Defendant violated the CMIA by disclosing its patients' medical information to Facebook and/or Google along with the patients' individually identifying information.

201. Plaintiff and Class Members seek nominal damages, compensatory damages, punitive damages, attorneys' fees, and costs of litigation for Defendant's violations of the CMIA.

FOURTH CAUSE OF ACTION
Violation of the Unfair Competition Law
(Cal. Bus. & Prof. Code § 17200, *et seq.*)
(On Behalf of Plaintiff and the California Class)

202. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

203. California's Unfair Competition Law ("UCL") prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

204. VSP engaged in unlawful business practices in connection with its disclosure of Plaintiff's and Class Members' Private Information to unauthorized third parties, including Facebook, in violation of the UCL.

205. VSP's acts, omissions, and conduct, as alleged herein, constitute "business practices" within the meaning of the UCL.

206. VSP violated the "unlawful" prong of the UCL by violating, *inter alia*, Plaintiff's and Class Members' constitutional rights to privacy, state and federal privacy statutes, and state consumer protection statutes.

207. VSP's acts, omissions, and conduct also violate the unfair prong of the UCL because those acts, omissions, and conduct offend public policy (including the federal and state privacy statutes and state consumer protection statutes, such as the ECPA, CIPA, CMIA, and HIPAA) and constitute immoral,

unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiff and Class Members.

208. The harm caused by VSP's conduct outweighs any potential benefits attributable to such conduct, and there were reasonably available alternatives to further VSP's legitimate business interests other than VSP's conduct described herein.

209. Plaintiff and Class Members suffered from a loss of the benefit of their bargain with VSP because they overpaid for insurance services they believed included data security sufficient to maintain their Private Information as confidential.

210. As a result of VSP's violations of the UCL, Plaintiff and Class Members are entitled to injunctive relief. This is particularly true since the dissemination of Plaintiff and Class Members' information is ongoing.

211. As result of VSP's violations of the UCL, Plaintiff and Class Members have suffered injury in fact and lost money or property, including but not limited to payments to VSP for services and/or other valuable consideration, *e.g.*, access to their private and personal data.

212. Plaintiff and Class Members would not have used VSP's services, or would have paid less for them, had they known VSP was breaching confidentiality and disclosing their Private Information to social media and tech giants, such as Meta, Microsoft, and Google.

213. The unauthorized access to Plaintiff's and Class Members' Private Information has also diminished the value of that information.

214. In the alternative to those claims seeking remedies at law, Plaintiff and Class Members allege that there is no plain, adequate, and complete remedy that exists at law to address VSP's unlawful and unfair business practices.

///

///

215. Further, no private legal remedy exists under HIPAA. Therefore, Plaintiff and Class Members are entitled to equitable relief to restore Plaintiff and Class Members to the position they would have been in had VSP not engaged in unfair competition, including an order enjoining VSP's wrongful conduct, restitution, and disgorgement of all profits paid to VSP as a result of its unlawful and unfair practices.

FIFTH CAUSE OF ACTION
Invasion of Privacy Under California's Constitution
(On Behalf of Plaintiff and the California Class)

216. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

217. Plaintiff and Class Members have an interest in: (1) precluding the dissemination and/or misuse of their Private Information; and (2) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various internet sites for the provision of insurance and health care without being subjected to wiretaps, pin registers, and/or trap and trace devices without their knowledge or consent.

218. By using Meta's Tracking Pixel to communicate patients' FIDs and other individually identifying information alongside their confidential medical communications and insurance information, VSP intentionally invaded Plaintiff's and Class Members' privacy rights under the California Constitution.

219. Plaintiff and Class Members had a reasonable expectation that their communications, identity, health information and other data would remain confidential, and that VSP would not install wiretaps, pin registers, and/or trap and trace devices to secretly transmit their communications and routing information.

///

220. Plaintiff and Class Members did not authorize VSP to transmit their Private Information to third parties, nor did they consent to allowing third parties to intercept, receive, and view those communications.

221. This invasion of privacy is serious in nature, scope, and impact because it relates to patients' private medical communications. Moreover, it constitutes an egregious breach of the societal norms underlying the privacy right.

222. As a result of VSP's actions, Plaintiff and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

223. Plaintiff and Class Members have been damaged as a direct and proximate result of VSP's invasion of their privacy and are entitled to just compensation, including monetary damages.

224. Plaintiff and Class Members seek appropriate relief for this injury, including but not limited to damages that will reasonably compensate them for the harm to their privacy interests.

225. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of VSP's actions, directed at injuring Plaintiff and Class Members in conscious disregard of their rights.

226. Such damages are needed to deter VSP from engaging in such conduct in the future.

227. Plaintiff also seeks such other relief as the Court may deem just and proper.

SIXTH CAUSE OF ACTION
Violation of the Electronic Communications Privacy Act
18 U.S.C. § 2510, *et seq*.
(On Behalf of Plaintiff and the Nationwide Class)

228. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

229. The Federal Wiretap Act ("FWA"), as amended by the Electronic Communications Privacy

///

Act of 1986 ("ECPA"), prohibits the intentional interception, use, or disclosure of any wire, oral, or electronic communication.

230. In relevant part, the ECPA prohibits any person from intentionally intercepting, endeavoring to intercept, or procuring "any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a).

231. The ECPA protects both sending and receipt of communications.

232. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

233. The transmissions of Plaintiff's Private Information via VSP's Web Properties qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(12).

234. **Electronic Communications**. The transmission of Private Information between Plaintiff and Class Members and VSP via its Web Properties are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

235. **Content.** The ECPA defines content, when used with respect to electronic communications, to "include[] *any* information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (emphasis added).

236. **Interception.** The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents … include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

///

///

237. **Electronic, Mechanical, or Other Device**. The ECPA defines "electronic, mechanical, or other device" as "any device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

(a) Plaintiff's and Class Members' browsers;

(b) Plaintiff's and Class Members' computing devices and mobile devices;

(c) VSP's web-servers; and

(d) The Tracking Tools deployed by VSP to effectuate the sending and acquisition of patient communications

238. When Plaintiff and Class Members interacted with VSP's Web Properties, VSP, through the Tracking Tools embedded and operating on its Web Properties, contemporaneously and intentionally disclosed, used, and redirected, and endeavored to disclose, use, and redirect, the contents of Plaintiff's and Class Members' electronic communications to third parties, including Facebook and Google, without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(c)-(d).

239. VSP's intercepted communications include, but are not limited to, the contents of communications to/from Plaintiff and Class Members regarding PII and PHI.

240. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiff and Class Members to Facebook, Google, and Microsoft, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), VSP violated 18 U.S.C. § 2511(1)(c)-(d).

241. VSP intentionally used the wire or electronic communications to increase its profit margins, and it specifically used the Tracking Tools to track and utilize Plaintiff's and Class Members' PII and PHI for financial gain.

242. VSP was not acting under color of law to intercept Plaintiff's and Class Members' wire or electronic communication.

243. Plaintiff and Class Members did not authorize VSP to acquire the content(s) of their communications via the Tracking Tools for purposes of invading their privacy.

244. Any purported consent VSP received from Plaintiff and Class Members was not valid.

245. **Unauthorized Purpose**. VSP intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious or criminal act in violation of the Constitution or laws of the United States or of any State – namely, violations of HIPAA, breaches of confidence, invasion of privacy, among others.

246. The ECPA provides that a "party to the communication" may be liable where a "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C § 2511(2)(d).

247. VSP is a "party to the communication" with respect to Plaintiff's and Class Members' communications, but its simultaneous, unknown duplication, forwarding, and interception of Plaintiff's and Class Members' Private Information does not qualify for the party exemption.

248. More specifically, VSP's acquisition of Plaintiff's and Class Members' communications, which were used and disclosed to unauthorized third parties, was done for the purpose of committing criminal and tortious acts in violation of the laws of the United States and California, including:

a) 42 U.S.C. § 1320d-6;

b) 45 CFR § 164.508(a)(1);

c) 15 U.S.C. § 45;

d) Cal. Penal Code § 631, *et seq*.;

e) Cal. Penal Code §638.51(a);

f) Cal. Civ. Code § 56, *et seq.*;

g) Cal. Bus. & Prof. Code § 17200; and

h) The common law causes of action alleged herein.

249. Under 42 U.S.C. § 1320d-6, it is a criminal violation for a person to "use[] or cause[] to be used a unique health identifier" or to "disclose[] individually identifiable health information to another person … without authorization" from the patient.

250. The penalty for violation is enhanced where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." 42 U.S.C. § 1320d-6.

251. VSP's conduct violated 42 U.S.C. § 1320d-6 in that it:

(a) Used and caused to be used persistent identifiers associated with specific patients without patient authorization; and

(b) Disclosed individually identifiable health information to Facebook and Google without patient authorization.

252. VSP's conduct would be subject to the enhanced provisions of 42 U.S.C. § 1320d-6 because VSP's use of the Tracking Technology was for its commercial advantage to increase revenue from existing patients and gain new patients.

253. VSP is not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d) on the ground that it was a participant in Plaintiff's and Class Members' communications because VSP used its participation in these communications to improperly share Private Information with third-parties that did not participate in these communications (Meta, Google, and LinkedIn) when Plaintiff and Class Members: (1) were unaware those third parties would receive their Private Information; and (2) did not consent to them receiving their Private Information.

254. VSP accessed, obtained, and disclosed Plaintiff's and Class Members' Private Information for the purpose of committing the crimes and torts described herein because it would not have been able to obtain the information or the marketing services if it had complied with the law.

255. As such, VSP cannot viably claim any exception to ECPA liability.

256. Plaintiff and Class Members have suffered damages as a direct and proximate result of VSP's invasion of privacy.

257. As a result of VSP's violation of the ECPA, Plaintiff and Class Members are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000, equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

SEVENTH CAUSE OF ACTION
Common Law Invasion of Privacy – Intrusion Upon Seclusion
(On Behalf of Plaintiff and the Nationwide Class)

258. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

259. Plaintiff and Class Members had a reasonable expectation of privacy in their communications with VSP via its Web Properties.

260. Plaintiff and Class Members communicated sensitive and protected medical information and individually identifiable information that they intended for only VSP to receive and which they understood VSP would keep private as their insurance provider and healthcare provider.

261. VSP's disclosure of the substance and nature of Plaintiff's and Class Members' communications to third parties without their knowledge and consent is an intentional intrusion on Plaintiff's and Class Members' solitude or seclusion.

262. Plaintiff and Class Members had a reasonable expectation that their communications,

identity, health information and other data would remain confidential, and that VSP would not install: (1) wiretaps to secretly transmit their communications to unauthorized third parties; or (2) pin registers and/or trap and trace devices.

263. VSP was authorized to receive Plaintiff's and Class Members' Private Information, but it was not authorized to: (1) commandeer Plaintiff's and Class Members' web browsers and devices, thereby forcing those devices to transmit information to Facebook, Google, and/or other third parties without their consent or authorization; or (2) divulge the Private Information via Meta's Conversions API and other server-to-server Tracking Tools.

264. As such, VSP obtained Plaintiff's and Class Members' Private Information under false pretenses and/or exceeded its authority to obtain the Private Information.

265. As a result of Defendant's actions, Plaintiff and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

266. Plaintiff and Class Members have been damaged as a direct and proximate result of VSP's invasion of their privacy and are entitled to just compensation, including monetary damages.

267. Plaintiff and Class Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests.

268. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of VSP's actions, directed at injuring Plaintiff and Class Members in conscious disregard of their rights. Such damages are needed to deter VSP from engaging in such conduct in the future.

269. Plaintiff also seeks such other relief as the Court may deem just and proper.

///

///

EIGTH CAUSE OF ACTION
Common Law Invasion of Privacy – Publication of Private Facts
(On Behalf of Plaintiff and the Nationwide Class)

270. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

271. Plaintiff's and Class Members' Private Information, including their communications and sensitive data, are private facts that third parties acquired without the knowledge or consent of Plaintiff and Class Members.

272. Defendant gave publicity to Plaintiff's and Class Members' Private Information and the content of their communications by sharing them with unauthorized third parties, including Meta, Google, and Microsoft, each of whom build massive databases of individual consumer profiles from which to sell targeted advertising and make further disseminations.

273. Plaintiff and Class Members did not know that VSP was using software to track and disclose their Private Information.

274. VSP's surreptitious tracking and commoditization of Plaintiff's and Class Members' Private Information is highly offensive to a reasonable person, particularly given that VSP provides vision insurance, partners with healthcare providers to offer medical services, and is engaged in the business of owning and operating vision clinics.

275. In disseminating Plaintiff's and Class Members' personal information without their consent, VSP acted with oppression, fraud, or malice.

276. Plaintiff and Class Members have been damaged by the publication of their Private Information and are entitled to just compensation in the form of actual damages, general damages, unjust enrichment, nominal damages, and punitive damages.

///

NINTH CAUSE OF ACTION
Common Law– Breach of Confidence

277. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

278. Plaintiff and Class Members disclosed their Private Information in confidence with VSP through VSP's Web Properties.

279. Plaintiff and Class Members have an interest in keeping their protected private and medical information confidential.

280. The information disclosed in confidence is protected health and private information the Defendant had knowledge was confidential due to Federal and State laws that protect such information (i.e., CIPA and HIPAA).

281. Plaintiff and Class Members had an expectation that the confidential information disclosed to Defendant would be kept in confidence with Defendant due to their relationship with Defendant as a health services provider and Federal and State laws that protect such information (e.g., CIPA, CMIA, and HIPAA).

282. VSP violated its duty to protect the confidentiality of Plaintiff's and Class Members' information by using Tracking Tools to communicate patients' Private Information with unauthorized third parties.

283. VSP disclosed Plaintiff's and Class Members' confidential information for VSP's own economic benefit in VSP's own business and disclosing it without Plaintiff's and Class Members' consent.

284. VSP disclosed and disseminated Plaintiff's and Class Members confidential communications to a broad audience including, Facebook, Google, and others.

285. At no time did VSP offer to purchase or financially compensate Plaintiff and Class

///

Members for the use of their confidential information for VSP's advertisement purposes.

286. As a result of VSP's actions, Plaintiff and Class Members suffered harm and injury, including but not limited to a breach of their confidence, were damaged as a direct and proximate result of VSP's breach, and are entitled to just compensation, including monetary damages.

287. Plaintiff also seeks such other relief as the Court may deem just and proper.

RELIEF REQUESTED

Plaintiff, on behalf of himself and the proposed Class, respectfully requests that the Court grant the following relief:

(a) Certification of this action as a class action and appointment of Plaintiff and Plaintiff's counsel to represent the Class;

(b) A declaratory judgement that Defendant violated: (1) the Electronic Communications Privacy Act; (2) the California Invasion of Privacy Act; (3) the California Confidentiality of Medical Information Act; (4) the Unfair Competition Law; (5) Plaintiff's and Class Members' privacy rights as provided at common law and pursuant to the California Constitution; and (6) Plaintiff's and Class Members' other rights under common law;

(c) An order enjoining VSP from engaging in the unlawful practices and illegal acts described herein; and

(d) An order awarding Plaintiff and the Class: (1) actual or statutory damages; (2) punitive damages—as warranted—in an amount to be determined at trial; (3) prejudgment interest on all amounts awarded; (4) injunctive relief as the Court may deem proper; (5) reasonable attorneys' fees and expenses and costs of suit pursuant to Cal. Code of Civil Procedure § 1021.5 and/or other applicable law; (6) pre-judgment and post-judgment interest as provided by law; and (7) such other and further relief as the Court may deem appropriate.

DEMAND FOR JURY TRIAL

Plaintiff, individually and on behalf of the proposed Class, demands a trial by jury for all the claims asserted in this Complaint so triable.

Date: March 6, 2025,

Respectfully submitted,

/s/ John J. Nelson
John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
402 W. Broadway, Suite 1760
San Diego, CA 92101
Telephone: (858) 209-6941
Fax: (865) 522-0049
Email: jnelson@milberg.com

/s/ Daniel O. Herrera
Daniel O. Herrera (*pro hac vice* forthcoming)
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
Email: dherrera@caffertyclobes.com

Counsel for Plaintiff and the Putative Class